

Hardening Windows 2000 in the Enterprise Part Two: Seeing the Forest in Spite of the Trees

Tim Mullen 2001-06-11

Hardening Windows 2000 in the Enterprise Part Two: Seeing the Forest in Spite of the Trees

by *Tim Mullen*

last updated June 11, 2001

This is the second article in a three-part series devoted to hardening Windows 2000 across the enterprise, as opposed to focusing on individual servers or workstations. In the [first installment](#), I discussed some of the security-enhancing tools that Windows 2000 offers, such as: Active Directory, Organizational Units, Security and Group Policies, and Security Configuration and Analysis. This article takes us right to the security policy options that can be used to strengthen our Win2k installations.

When I first began working with these options in Win2k, I was confused. I probably could have read through the help files, but I tend to attack new features like this as if they were bots in a Quake level: I jump in and start shooting. Right off the bat, I was presented with many options: I could set policy via the Domain Security Policy, Domain Controller Security Policy, or the Local Security Policy. The Domain Security Policies had a few more options than the LSP did, and I was not sure why. More exploration led me to the Group Policy options, which allowed even more configuration settings to be made (we'll cover the Group Policy stuff next time). I wasn't really sure what to do where, and was still trying to figure out why to do it in the first place.

I eventually downloaded [Group Policy](#) and [Security Configuration](#) white papers from the Microsoft web site, only to find that much of the content still referred to Beta and to-be-implemented options. While the documents were helpful, some of the errant content, such as references to Beta options and no-longer-valid naming conventions was not so helpful. After a fair bit of experimentation, I have finally arrived at a point at which I thought that I had a pretty good grasp on the entire structure, and really feel good about deploying custom configurations throughout my enterprise. If the dissemination of this information can save even one of you a little time, then I have done my job.

This can get a bit "fangy", (as in something with big nasty fangs) so be patient. OK, I know that

"fangy" isn't a real word, but I figure if I use it enough, it will eventually become one, and I will finally get credit for the time I used it in a Scrabble game against Mike Parnell. Besides, it is apropos. So, here we go?

The Local Security Policy node contains 3 main areas where you can set policy options: Account Policies, Local Policies, and Public Key Policies. Once you get these down, you will see that you can then apply them at the Domain, Domain Controller, Site, or Organizational Unit levels (Note that the Kerberos Policy, a subset of the Account Policies, is only for domain accounts, even if set in a local policy, unless of course the local system is a DC. But you knew that). These system-specific options (as opposed to user-specific) can be set either directly in the LSP MMC, via an imported template, through the Security Configuration and Analysis Tool, or as part of a group policy. This also happens to be the proposed method of securing Internet-facing boxes that a team working with the [Center for Internet Security](#) is currently developing.

For your reading pleasure, I have compiled the complete list of options that can be set, along with a brief description of each option, based on the Microsoft white papers. I have also included my recommendations for some of the settings, based on my experience; but make sure you check these options out before you simply set them - I would hate to see you break anything! Finally, there will be a <.02> tag under the MS description, in which I have inserted my own comments - my own two cents worth, as it were.

Note that in some cases, I have used 'Not Defined' as my recommended setting, which means I have refrained from suggesting a setting. This could be because it is essentially a matter of individual preference, because it is based on other settings, or because I simply don't know enough about it to make recommendations. 'Not Defined' is quite different than 'Disabled'. A 'Disabled' policy is explicitly defined as not engaged, or is turned off. Also, note that the following explanations are not exhaustive: they have been summarized (and generalized) for the sake of brevity, and are offered as a reference. For more in-depth explanations, readers should refer to the original Microsoft white papers.

Account Policies - Password Policy, Account Lockout Policy, and Kerberos Policy

Password Policy

<.02>

Good passwords are the first step to securing your network. While Win2k now uses Kerberos, don't think that LM is dead and gone - there are still ways to revive that zombie, so it is best to keep your guard up. More on this below.

</.02>

Enforce password history

This policy keeps users from reusing passwords by keeping the password history according to the setting: someone could only reuse a password after changing it n times, where n equals the password history setting.

Author's recommended setting: 8

Maximum password age

The maximum number of days that a password can be used before a user must change it. The value can be between 1 and 999 (0 means that the passwords never expire.)

The GPO and LSA of workstations and servers sets the default to 42.

<.02>

I have seen recommendations from 30 to 120. There is no magic number - the thing to consider is how often you make users change passwords, how complex they have to be, and how much flack you will catch for making users do too much work. If the end result is a password written on a sticky note slapped up on the monitor, the policy has failed.

</.02>

Author's recommended setting: 90

Minimum Password Age

Sets the minimum time a password can be used before it can be changed. This must be less than the maximum password age.

The GPO and LSA of workstations and servers sets the default to 0, allowing immediate changes, so note this if you use Enforce Password History. Having a 0 allows users to keep changing the password to get back to one they want to effectively bypass history enforcement.

Author's recommended setting: Not Defined

Minimum password length

Enforces minimum password length in characters. A setting of 0 allows for a blank password, which is the default for the GPO and the LSA in workstations and servers.

<.02>

This is a hot topic. Now that we have Kerberos, why care about this 7- or 8-character password business? Well, because you can still force an LM connection to your box unless you otherwise disable it. Plus, the LM is still in the local SAM that was initially created, unless you specifically disable it via an undocumented registry setting. See Eric Schultze's article, [Choosing Strong Passwords](#) on the Security Focus web site.

</.02>

Author's recommended setting: 7

Passwords must meet complexity requirements

Forces password complexity, and is disabled by default. A complex password (as enforced by this setting's implementation of 'passfilt.dll') is one that:

- does not contain any part of the account name;
- is at least 6 characters in length; and,
- contains 3 out of 4 of character types of uppercase, lowercase, digits, and extended characters (like the shift of the upper number keys).

It is possible to create custom filters via the Platform SDK, though I have never done so.

Author's recommended setting: Enabled

Store password using reversible encryption for all users in the domain

For compatibility with third party SMB servers, you can choose to store your passwords in reversible encryption, which may as well be clear text. This should always be disabled unless you absolutely must enable it for application purposes.

Author's recommended setting: Disabled

Account Lockout Policy

Account lockout threshold

The number of times before a failed logon locks out an account. Upon lockout, an admin must clear the 'account locked out' flag, or the lockout duration period must expire. Valid arguments are between 1 and 999, as if anyone would actually set it to 999. A value of 0 will never lock out.

The setting is not enabled by default. Password protected screen saver attempts do not count, as you are not really logging on.

Author's recommended setting: 3

Account lockout duration

After failed logon attempts result in a lockout, this is the number of minutes before the account automatically clears itself, from 1 to 99999 minutes. 0 in this case means it will never unlock, and requires administrative clearing. This has to be greater than the reset time described below.

<.02>

I have seen smaller values than my recommended setting that are presumably set to save the user any extended down time while waiting for the reset. It has been my experience that the user never waits anyway, and will always contact an administrator. If it is on the weekend, you are going to get a page anyway, so you may as well set it pretty high to thwart automated/brute force attempts.

</.02>

Author's recommended setting: 90

Reset account lockout counter after

This is the number of minutes the system will wait before it resets the 'bad logon attempts'

back to 0. If you fat-finger a password, giving you one strike, then it will be set back to 0 after n minutes. It is not defined by default, as the Account Lockout Threshold must be set for it to be useful.

Author's recommended setting: 30 minutes

Kerberos Policy

These options are all set by default in the Default Domain Controller GPO, and that is how I leave them. Others with more experience in the Kerberos arena, please share any insight with [me](#).

Enforce user logon restrictions

When enabled, this makes the Kerberos KDC validate requests for sessions tickets against the local policies of the target system. It supposedly takes more resources for this action, though I have not tested it. The user must have 'Log on Locally' or 'Access this computer' from the Network rights to receive the ticket.

Author's recommended setting: enabled

Maximum lifetime for service ticket

This setting regulates the maximum number of minutes that a session ticket is valid to access a service after being granted. This is for new connections only, not for sessions that have already been authenticated. This setting must be more than 10 minutes, and equal to or less than the User Ticket setting.

Author's recommended setting: 600 minutes

Maximum lifetime for user ticket

Time (in hours, not minutes? why the inconsistency?) that the ticket-granting ticket is valid. This setting is set to 10 hours in GPO by default.

Author's recommended setting: 10 hours

Maximum lifetime for user ticket renewal

The threshold (in days) in which the ticket-granting ticket can be renewed.

This setting is set to 7 days in the GPO by default.

Author's recommended setting: 7 days

Maximum tolerance for computer clock synchronization

Differences in client and server time can make Kerberos authentication fail, as part of the way the protocol works. This setting determines the time differential tolerance. It is set to 5 as the default in the GPO.

Author's recommended setting: 5 minutes

Local Policies - Audit Policy, User Right Assignment, and Security Options

Audit policy

Auditing does absolutely no good unless the logs are reviewed by administrative personnel. This is particularly true for the following settings, which assume 'overwrite the logs as necessary' is set. Note that the Event Log properties of the Domain Security Policy GPO define the event log settings, not the Local Security Policy. The Domain (or equivalent OU Policy) should be used for this.

Audit account logon events

This audits when the system with this setting does or doesn't log a user on or off, depending on the setting. The default is 'No Auditing'.

<.02>

I like to log success as well as failure. Not just for identifying those 3:00 AM admin logons, but for general troubleshooting as well.

</.02>

Author's recommended setting: Success and Failure

Audit account management

Sets what type of event to audit when account management functions are executed on a system, such as user creation or deletion, password changes, etc. The default setting is 'No Auditing'.

Author's recommended setting: Success and Failure

Audit directory service access

Sets how to log Active Directory objects with System Access Control Lists (SACLs). This is similar to Audit Object Access, except this is at the AD level.

Author's recommended setting: Failure

Audit logon events

Audits when a user makes a network connections to this system, or logs on or off to this system. Unlike Account Logons, which take place at the DC or authenticating unit, this audits when the system itself is accessed.

Author's recommended setting: Failure

Audit object access

Sets the audit type for objects (files, directories, registry keys, etc.) Note that you must also go to the object and set the SACL for the object you wish to audit.

<.02>

I use this off and on, mostly for specific troubleshooting issues where I want to see how the objects are being accessed. Some people leave this on all the time, and only set auditing on specific objects when they need to. Some have said that this consumes system resources, but I have seen no evidence of that. I left this at 'Not Defined' so that you can make your own decision of how to go about doing this.

</.02>

Author's recommend setting: Not Defined

Audit policy change

Sets the audit type for changes in user right policy, trust policies, or audit policies themselves.

<.02>

It is important to know when audit policy changes succeed, as a successful change could stop auditing in the first place. If you only audit failure, you may not catch strange activity.

</.02>

Author's recommended setting: Success and Failure

Audit privilege use

Determines the audit type when users exercise their user rights. According to the help files, the following are not logged, even when success or failure is requested:

- bypass traverse checking;
- debug programs;
- create a token object;
- replace process level token;
- generate Security Audits;
- backup files and directories; and,
- restore files and directories;

<.02>

I have left systems with 'Failure Logging' on, but it really seems to generate a lot of extraneous log entries that are not self explanatory, almost to the point of creating a smoke screen effect - even with Admin users you stop really paying attention to them. If others have some insight into the proper use for this, I would like to know about it, please.

</.02>

Author's recommended setting: Not Defined

Audit process tracking

Audits program activation, process exits and stuff like that. This is like the Object Access: I use it for specific troubleshooting or process tracking, but don't keep it on all the time.

Author's recommended setting: Not Defined

Audit system events

Sets the audit type for when a system is shut down or restarted, or where events that affect the system or security log occur. Determines whether to audit when a user restarts or shuts down the computer, or when an event has occurred that affects either the system security or the security log.

<.02>

It might just be me, but I like to know when systems are restarted, or when the security log is affected by something. I log success and failure for that reason.

</.02>

Author's recommended setting: Success and Failure

User Rights Assessment

Access this computer from network

Sets who can connect to the system over the network. The defaults are too lenient, and I recommend that you change it to 'Authenticated Users' at least. It would be far better to build a group policy that makes for easy administration, and only grants access to a custom group.

Author's recommended setting: Authenticated Users

Act as part of the operating system

I recommend that this be given to the 'Everyone' group. Just kidding! I was checking to see if you were still paying attention.

This gets a bit complicated, but it basically allows you to give a process complete access to the system. This can result in custom token generation and all that jazz. That is why LocalSystem is

the default. The recommendation is to have processes that need this use LocalSystem rather than giving the process itself this right.

Author's recommended setting: LocalSystem

Add workstations to domain

Valid only on a DC, this policy allows you to determine which users or groups can add workstations to the domain, by way of creating a computer account. Fortunately, only 10 accounts can be added (by default) by the "authenticated user", so you don't have to worry about an Account Stuffing that could bring down AD.

<.02>

Even though only 10 accounts can be added, you should still be careful who you give this right to - I don't know of any valid reason why you would want just anyone to be able to add a computer account to your domain.

</.02>

Author's recommended setting: Other than Authenticated Users

Backup files and directories

This setting determines who can perform backups. Permissions are bypassed during this operation, so the default is Admin and Backup Operators.

<.02>

The defaults let the same person backup and restore, if they are part of the Backup Operators group. This is not so smart because I can effectively bypass permissions to get to a file if I can back it up and then restore it again somewhere else. Let people back it up, but have different user accounts restore it.

</.02>

Author's recommended setting: Administrators/Backup Operators

Bypass traverse checking

This setting determines which accounts can traverse a directory, even if they do not

permissions for that directory. They can't access the contents, they can only move through it.

Author's recommended setting: Not Defined

Change the system time

Sets who can change the system time. Since Kerberos authentication can be disabled if the threshold is exceeded, you want to limit who can do this, as alternate authentication methods can be used on failure.

Author's recommended setting: Administrators

Create a pagefile

This setting determines who can create or change pagefile settings. The default is Administrators.

Author's recommended setting: Administrators

Create a token object

Token creation allows access resources, so the recommendation is to keep this at LocalSystem. If other processes can create tokens, then there could be security problems. If you must create tokens, then do so under LocalSystem, don't set your process here.

Author's recommended setting: LocalSystem

Create permanent shared objects

This doesn't govern who can share resources, it sets what accounts a process can use to create Object Manager objects. This is kernel mode stuff, so leave it alone.

Author's recommended setting: LocalSystem

Debug programs

People who can debug programs have access to special system information. You should leave

this set as the default, which is Administrators and LocalSystem.

Author's recommended setting: Administrators/LocalSystem

Deny access to this computer from the network

Specifically denies access from the network. All other permissions are ignored if 'Deny' is in place. This is not defined by default.

<.02>

This can be a powerful setting. Typically, service accounts are created locally for security reasons. However, if you use domain accounts that are part of a special group, that group can be denied access over the network to all other systems. 'Deny' supercedes all other explicit access. It is a bit tricky, and goes against some recommended procedures, but the new Group Policy management allows pretty easy administration of this, and it can provide a decent amount of security.

</.02>

Author's recommended setting: Not Defined

Deny logon as a batch job

Explicitly denies an account the 'Logon as Batch Job' privilege (See 'Logon as Batch Job' for more info.)

Author's recommended setting: Not Defined

Deny logon as a service

Explicitly denies an account the 'Logon as Service' privilege (See 'Logon as Service' for more info.)

Author's recommended setting: Not Defined

Deny logon locally

Explicitly denies the 'Logon Locally' privilege (See 'Logon Locally'.)

Author's recommended setting: Not Defined

Enable computer and user accounts to be trusted for delegation

This allows user accounts to be trusted for delegation, meaning a process can access other resources on a different computer with the delegated credentials.

Author's recommended setting: Administrators

Force shutdown from a remote system

This setting determines which accounts can remotely shut down another system.

Author's recommended setting: Administrators

Generate security audits

Sets which accounts can be used by a process to add entries to the security log. The default is 'LocalSystem'.

Author's recommended setting: LocalSystem

Increase quotas

This setting determines which accounts can use processes that have 'write property' access to other processes in order to increase the processor quota. The setting is used to tune performance, but it can be used maliciously to peg processor utilization.

Author's recommended setting: Administrators

Increase scheduling priority

Determines who can increase the priority of a process. As with 'Increase Quotas', it can be used maliciously to peg processor utilization.

Author's recommended setting: Administrators

Load and unload device drivers

This setting determines which user accounts can load device drivers. Device drives run in kernel mode, and can be dangerous, such as a rootkit.

<.02>

Consider creating a custom group, and only populating it with the user accounts of select administrators and only granting this group this right. Yes, it is security through obscurity, but it may save your patooty. Guys like Greg Hoggund and JD Glaser have some pretty cool kits that dynamically load without a reboot if you let them?

</.02>

Author's recommended setting: Administrators

Lock pages in memory

Determines which user accounts can keep data in physical memory, and not page to disk. Can affect performance.

Author's recommended setting: Not Defined

Logon as a batch job

Specifies which users can logon as a batch job, as in a task scheduler job. 'Local System' is the default.

Author's recommended setting: LocalSystem

Logon as a service

Determines which accounts can be used to run a service. By default, no accounts have this right, but they are automatically given the right when you select a user account for a service to run under.

Author's recommended setting: Not Defined

Logon locally

This setting determines who may log on locally (interactively) to the system.

Author's recommended setting: Not Defined

Manage auditing and security log

Determines who can manage auditing and the security log options.

Author's recommended setting: Administrators

Modify firmware environment variables

Determines who can modify system environmental variables.

Author's recommended setting: LocalSystem

Profile single process

This setting determines which user accounts can use Performance Monitor to profile non-system processes.

Author's recommended setting: Administrators/LocalSystem

Profile system performance

Sets which user accounts can use Performance Monitor to profile system processes.

Author's recommended setting: Administrators/LocalSystem

Remove computer from docking station

This setting determines which users can undock a laptop from its docking station (logically, of course). Upgrades to Win2k require explicit user rights to be given for this setting.

Author's recommended setting: Not Defined

Replace a process level token

This setting determines which users can replace a processes default token. By default, only LocalSystem has this right.

Author's recommended setting: LocalSystem

Restore files and directories

This setting determines who can restore files and directories. These users bypass security settings, so make sure you don't give the same dude Backup as you do Restore.

Author's recommended setting: Administrators/Backup Operators

Shut down the system

This setting determines who can shut down the local system (gracefully!)

<.02>

Too bad there is not a 'Deny Pull the Plug Access' policy.

</.02>

Author's recommended setting: Not Defined

Take ownership of files or other objects

This setting determines which users can take ownership of system objects.

Author's recommended setting: Administrators

Security Options

Additional restrictions for anonymous access

Sets restrictions (kind of) for Null User access to system information. You can set the following restrictions:

- 'None'
- 'Do not allow enumeration of SAM accounts and shares' - supposedly replaces 'Everyone' with 'Authenticated Users' for the token.
- 'No access without explicit anonymous permissions' - removes 'Everyone' and 'Network' when the token is being generated. You must then explicitly grant that the null user be given access.

<.02>

If you can get away with 'No access', then do. Anything other than that, and intruders can still get all kinds of information from the system. This won't work with downlevel trusts or with NT workstations that must authenticate to the box. See the author's article [RestrictAnonymous: Enumeration and the Null User](#) for more info.

</.02<

Author's recommended setting: Not Defined

Allow server operators to schedule tasks (domain controllers only)

If enabled, this gives Server Operators the ability to submit jobs via AT (not the Task Scheduler).

Author's recommended setting: Administrators

Allow system to be shut down without having to log on

If enabled, this allows the system to be shutdown without logging in first.

Author's recommended setting: Not Defined

Allowed to eject removable NTFS media

Sets which users can eject removable media if formatted NTFS.

Author's recommended setting: Not Defined

Amount of idle time required before disconnecting a session

Sets the amount of time in minutes before a server will disconnect an inactive SMB session. 15 minutes is the default, and a 0 makes the session disconnect as soon as is possible.

Author's recommended setting: Not Defined

Audit the access of global system objects

Sets the audit policy for global system objects like semaphores, events and DOS devices. When enabled, the SACL's are automatically set to audit.

Author's recommended setting: Not Defined

Audit use of all user rights including Backup and Restore

Remember how Audit Privilege Use does not audit all events? This is a means of getting all events logged when a user exercises rights.

Author's recommended setting: Not Defined

Automatically log off users when logon time expires

This is a domain-wide setting (as opposed to the next policy's local-only influence) that will forcibly log out users when the logon time expires.

<.02>

I don't know too many admins that set this, due to the potential "freak-factor" that a user may experience, but it is really a powerful way to limit access. In fact, I would just be happy to see more people have logon times set in the first place for the user accounts?

</.02>

Author's recommended setting: Not Defined

Automatically log off users when logon time expires (local)

Same as above, except that disconnects local users from resources.

Author's recommended setting: Not Defined

Clear virtual memory pagefile when system shuts down

This setting, when enabled, forces the page file to be cleared (wiped clean) every time the system shuts down.

Author's recommended setting: Not Defined

Digitally sign client communications (always)

This sets how the client will attempt to digitally sign its communications. When set, it must always sign SMBs, thus preventing man-in-the-middle attacks. Note that you must also require it on the server if you want the client to communicate with it.

<.02>

The word is that this takes about 10% more CPU time on the client and server (when establishing the SMB communications), though I have not personally verified this. Even so, I think it is worth the overhead to secure the communications. I still leave this one as Not Defined so that you can make your own choice.

</.02>

Author's recommended setting: Not Defined

Digitally sign client communications (when possible)

Same as the previous policy, except that is a best effort. If signing can take place, it will, but it is not required.

<.02>

I recommend enabling this, but would really rather see it required; however, I don't want to see you break anything, so there you have it.

</.02>

Author's recommended setting: Enabled

Digitally sign server communications (always)

This requires that SMB communications be signed at the server at all times. See above for comments regarding signing.

Author's recommended setting: Not Defined

Digitally sign server communications (when possible)

Same as above, except that it will sign when it can, but it is not required.

Author's recommended setting: Enabled

Disable CTRL+ALT+DEL requirement for logon

Sets the requirement for the user to use C+A+D to log on.

<.02>

I guess this helps some, but this does nothing to stop kernel mode root kits or physical keyboard loggers from capturing logon creds. Your best bet is to leave this policy disabled (which still requires C+A+D.)

</.02>

Author's recommended setting: Not Defined

Do not display last user name in logon screen

By default, the last user account name is displayed in the logon screen. Enabling this policy required the username to be entered each time.

<.02>

Again, I guess this could help some, but if I have my hands on the box, then I own it, so don't take this too seriously. Besides, if you require the account name to be secret, you have bigger problems.

</.02>

Author's recommended setting: Not Defined

LAN Manager authentication level

This sets what LM authentication level will be used when LM is used to validate creds. Your choices are as follows:

- send LM & NTLM responses: Clients use LM and NTLM authentication, and never use NTLMv2 session security; DCs accept LM, NTLM, and NTLMv2 authentication.
- Send LM & NTLM - use NTLMv2 session security if negotiated: Clients use LM and NTLM authentication, and use NTLMv2 session security if server supports it; DCs accept LM, NTLM, and NTLMv2 authentication.
- Send NTLM response only: Clients use NTLM authentication only, and use NTLMv2 session security if server supports it; DCs accept LM, NTLM, and NTLMv2 authentication.
- Send NTLMv2 response only: Clients use NTLMv2 authentication only, and use NTLMv2 session security if server supports it; DCs accept LM, NTLM, and NTLMv2 authentication.
- Send NTLMv2 response only\refuse LM: Clients use NTLMv2 authentication only, and use NTLMv2 session security if server supports it; DCs refuse LM (accept only NTLM and NTLMv2 authentication).
- Send NTLMv2 response only\refuse LM & NTLM: Clients use NTLMv2 authentication only, and use NTLMv2 session security if server supports it; DCs refuse LM and NTLM (accept only NTLMv2 authentication).

The default is "Send LM & NTLM responses."

<.02>

You can still force a box to use LM in different ways. I suggest 'Use v2 if negotiated' so as not to break anything, but you should see if you can get away with at least NTLM or v2 if possible. You'll have to get the client drivers for Win9x to use NTLMv2. This requires some work on your part to test.

</.02>

Author's recommended setting: Send LM & NTLM - Use v2 if neg.

Message text for users attempting to log on

This specifies what text to display when a user begins the logon process.

<.02>

Here is my logon text, which is pretty good. I got it from the Department of Energy:

"This is a private computer system and is the property of [Company]. It is for authorized use only. Users (authorized or unauthorized) have no explicit or implicit expectation of privacy. Any or all uses of this system and all files on this system may be intercepted, monitored, recorded, copied, audited, inspected, and disclosed to authorized site personnel, law enforcement personnel, as well as authorized officials of other agencies. By using this system, the user consents to such interception, monitoring, recording, copying, auditing, inspection, and disclosure at the discretion of authorized [Company]. personnel. Unauthorized or improper use of this system may result in administrative disciplinary action and civil and criminal penalties. By continuing to use this system you indicate your awareness of and consent to these terms and conditions of use. LOG OFF IMMEDIATELY if you do not agree to the conditions stated in this warning."

Of course, the user doesn't really have to hit "OK"? They can just wait a few minutes and the message goes away by itself, so I am just waiting for the legal ramifications of the fact that it would be possible for the user to continue without acknowledgement.

</.02>

Author's recommended setting: Legal Notice (clear with your corporation or organization)

Message title for users attempting to log on

Sets the title bar for the above notice.

<.02>

I've been told that the words "Legal Notice" have some binding power?

</.02>

Author's recommended setting: Legal Notice title (clear with your corporation or organization)

Number of previous logons to cache (in case domain controller is not available)

Sets how many logon credentials will be cached in case a DC cannot be reached. The default is 10 with a max of 50. 0 disables caching altogether. Cached creds are a security concern.

Author's recommended setting: Not Defined

Prevent system maintenance of computer account password

Computer account passwords are automatically reset each week by default. If you have some reason that you do not want a computer's account password to be reset, you can enable this policy, but it is not recommended.

Author's recommended setting: Disabled

Prevent users from installing printer drivers

Just like device drivers, printer drivers run in kernel mode. This policy keeps users from loading printer drivers on workstations, where they have the default right to do so (not on servers). Unfortunately, anyone on a workstation can add printer drivers.

<.02>

Printer drivers are great places to hide root kits and Trojans for this reason. Be careful where you let users load drivers, and where they get drivers from. See "Unsigned Driver Behavior" for more options.

</.02>

Author's recommended setting: Not Defined

Prompt user to change password before expiration

With a default of 14 days, this option allows you to set how far in advance the system warns a user that their password is about to expire.

Author's recommended setting: Not Defined

Recovery Console: Allow automatic administrative logon

This policy allows you to automatically log on to the system Recovery Console when set. This is obviously unsafe, but may be necessary, depending on your environment.

Author's recommended setting: Not Defined

Recovery Console: Allow floppy copy and access to all drives and folders

Enables the following Recovery Console SET commands: (from the Microsoft Help Documents)

- AllowWildCards - Enable wildcard support for some commands (such as the DEL command).
- AllowAllPaths - Allow access to all files and folders on the computer.
- AllowRemovableMedia - Allow files to be copied to removable media, such as a floppy disk.
- NoCopyPrompt - Do not prompt when overwriting an existing file.

These SET commands are disabled, and all these variables are not enabled by default.

Author's recommended setting: Not Defined

Rename administrator account

Sets, as a matter of policy, whether or not the admin account must be renamed.

<.02>

This is really only valuable for Terminal Server, where the TS logon is local - you can't lock out the admin account from a local logon, so a BF attack against TS is possible. Determining the real administrator account name on any box that you can hit with 139 is trivial.

</.02>

Author's recommended setting: Not Defined

Rename guest account

Sets, as a matter of policy, whether or not you must rename the guest account. See the previous policy for obscurity comments.

Author's recommended setting: Not Defined

Restrict CD-ROM access to locally logged-on user only

Sets whether or not the CD is available to local and network users.

Author's recommended setting: Not Defined

Restrict floppy access to locally logged-on user only

Sets whether or not the floppy CD is available to local and network users.

Author's recommended setting: Not Defined

Secure channel: Digitally encrypt or sign secure channel data (always)

This setting will make the system require that all secure channels be signed or encrypted. All DC's in all domains must share this setting, if specified. Enabling this setting automatically enables the 'Digitally sign secure channel (when possible)' setting.

Author's recommended setting: Not Defined

Secure channel: Digitally encrypt secure channel data (when possible)

Same as above, except that it is a best effort without requiring the channel be signed or encrypted.

Author's recommended setting: Enabled

Secure channel: Digitally sign secure channel data (when possible)

Sets whether outgoing secure channel data should be signed or not.

Author's recommended setting: Enabled

Secure channel: Require strong (Windows 2000 or later) session key

This requires that all secure channel data have a strong encryption key (Win2k+ only.)

Author's recommended setting: Not Defined

Secure system partition (for RISC platforms only)

Restricts access to the FAT system partition on RISC boxes to admin only (while the OS is running).

Author's recommended setting: Not Defined

Send unencrypted password to connect to third-party SMB servers

This setting allows you to send your creds in the clear to 3rd party SMB servers.

Author's recommended setting: Disabled

Shut down system immediately if unable to log security audits

This setting allows you to make the system halt should it not be able to log a security event with a **Stop: C0000244** code.

<.02>

I'm a little bittersweet about this one. I would love to have the system automatically shut down if security log entries flooded it to the point that it could not log anymore, but I just don't trust it. Talk about a self-imposed denial of service!

</.02>

Author's recommended setting: Not Defined

Smart card removal behavior

Sets what action you want the system to take when a logged-on user yanks the smart card. You can choose from No Action, Lock Workstation, or Force Logoff.

Author's recommended setting: Enabled

Unsigned driver installation behavior

This allows you to lock down the installation of unsigned drivers. Your choices are: Silently Succeed, Warn by allow, or Do not allow installation.

<.02>

If you can get away with it, don't allow the installation of unsigned drivers. Users should not be loading drivers anyway. That could lead to problems though, so think it through before just setting it.

</.02>

Author's recommended setting: Not Defined

Unsigned non-driver installation behavior

Same as above, but for non-driver software.

Author's recommended setting: Not Defined

A few final words

So, is anyone still with me? I know that was a lot of material to cover, but we are only getting started! Next time, we will go into even more detail about the user options that can be set (and some tips on how to set them) with Group Policies.

If you want to get a jump on that and check out the Microsoft white papers that I used as the basis for this article, take a look at [Windows 2000 Group Policy](#) as well as [Security Configuration and Analysis](#) for the skinny on the Security Configuration and Analysis tools.

Until then?

To read **Hardening Windows 2000 in the Enterprise: Seeing the Forest in spite of the trees, Part III**, click [here](#).

[Privacy Statement](#)

Copyright 2006, SecurityFocus