



Introduction

This document specifies the organisation's standard security template settings for computers running Microsoft Windows 2000 Server.

Templates may be applied to target computers in one of two ways: by importing them into a Group Policy Object and using Group Policy for distribution, or by importing them directly into the Local Security Settings of each machine.

These standard template settings should be thoroughly tested before implementation on live systems.



Domain-Wide Policies

Domain Password Policy

- Set the following Password Policy in *Account Policies\Password Policy*:

Policy	Default setting	Recommended setting
Enforce password history	0 passwords remembered	13 passwords remembered
Maximum password age	42 days	30 days
Minimum password age	0 days	1 day
Minimum password length	0 characters	7 characters
Passwords must meet complexity requirements	Disabled	Enabled
Store password using reversible encryption for all users in the domain	Disabled	Disabled

- Poor quality passwords are a serious problem within many organisations. There are two ways to counter this vulnerability: by educating users to comply with the organisation's published policy on password construction, and by enforcing this policy using technical means. A combination of both approaches is recommended. It should be noted that enabling *Passwords must meet complexity requirements* requires passwords to be constructed from any three of lower case, upper case, numeric and symbol characters, and disallows passwords related to the user name. This is likely to result in some additional administrative overhead, at least in the early stages of implementation.

Domain Account Lockout Policy

- Set the following Account Policy in *Account Policies\Account Lockout Policy*:

Policy	Default setting	Recommended setting
Account lockout duration	Not defined	0
Account lockout threshold	0	3 invalid logon attempts
Reset account lockout counter after	Not defined	1440 minutes (= 24 hours)



Domain Controller Policies

Domain Controller Audit Policy

- Set the following Audit Policy in *Local Policies\Audit Policy*:

Policy	Default setting	Recommended setting
Audit account logon events	No auditing	Success, Failure
Audit account management	Not defined	Success, Failure
Audit directory service access	No auditing	Failure
Audit logon events	No auditing	Success, Failure
Audit object access	No auditing	Failure
Audit policy change	No auditing	Success, Failure
Audit privilege use	No auditing	Failure
Audit process tracking	No auditing	No auditing
Audit system events	No auditing	Success, Failure

- Note that enabling auditing for object access does not in itself cause any auditing of objects. Rather it *enables the possibility* of object auditing, which then requires specific objects (e.g. files, folders) to have auditing enabled for specific users or groups in order to generate events in the Security Event Log.

Domain Controller User Rights Assignment

- Set the following User Rights Assignment in *Local Policies\User Rights Assignment*:

Policy	Default setting	Recommended setting
Access this computer from the network	Administrators, Authenticated Users, Everyone	Administrators, Authenticated Users
Act as part of the operating system		None
Add workstations to domain	Authenticated Users	Administrators
Back up files and directories	Administrators, Backup Operators, Server Operators	Backup Operators
Bypass traverse checking	Administrators, Authenticated Users,	Administrators, Backup Operators, Server

Windows 2000 Security Templates



	Everyone	Operators
Change the system time	Administrators, Server Operators	Administrators
Create a pagefile	Administrators	Administrators
Create a token object		None
Create permanent shared objects		
Debug programs	Administrators	None
Deny access to this computer from the network		None
Deny logon as a batch job		
Deny logon as a service		
Deny logon locally		
Enable computer and user accounts to be trusted for delegation	Administrators	
Force shutdown from a remote system	Administrators, Server Operators	Administrators
Generate security audits		
Increase quotas	Administrators	Administrators
Increase scheduling priority	Administrators	Administrators
Load and unload device drivers	Administrators	Administrators
Lock pages in memory		None
Log on as a batch job		
Log on as a service		Replicators
Log on locally	Account Operators, Administrators, Backup Operators, Server Operators, Print Operators	Administrators, Backup Operators, Server Operators
Manage auditing and security log	Administrators	Administrators
Modify firmware environment values	Administrators	Administrators
Profile single process	Administrators	Administrators
Profile system performance	Administrators	Administrators
Remove computer from docking station	Administrators	Administrators
Replace a process level token		None
Restore files and directories	Administrators, Backup Operators, Server	Backup Operators



	Operators	
Shut down the system	Account Operators, Administrators, Backup Operators, Server Operators, Print Operators	Administrators, Server Operators
Synchronize directory service data		
Take ownership of files or other objects	Administrators	Administrators

- *None* means that no users or groups must be granted the privilege

Domain Controller Security Options

- Set the following Security Options in *Local Policies\Security Options*:

Policy	Default setting	Recommended setting
Additional restrictions for anonymous connections	None. Rely on default permissions	No access without explicit anonymous permissions
Allow server operators to schedule tasks (domain controllers only)	Not defined	Not defined
Allow system to be shut down without having to log on	Disabled	Disabled
Allowed to eject removable NTFS media	Administrators	Administrators
Amount of idle time required before disconnecting session	15 minutes	15 minutes
Audit the access of global system objects	Disabled	Enabled
Audit use of Backup and Restore privilege	Disabled	Enabled
Automatically log off users when logon time expires	Not defined	Enabled
Automatically log off users when logon time expires (local)	Enabled	Enabled
Clear virtual memory pagefile when system shuts down	Disabled	Enabled
Digitally sign client communication (always)	Disabled	Disabled

Windows 2000 Security Templates



Digitally sign client communication (when possible)	Enabled	Enabled
Digitally sign server communication (always)	Disabled	Disabled
Digitally sign server communication (when possible)	Enabled	Enabled
Disable CTRL+ALT+DEL requirement for logon	Disabled	Disabled
Do not display last user name in logon screen	Disabled	Enabled
LAN Manager Authentication Level	Send LM & NTLM responses	Send NTLM response only
Message text for users attempting to log on		<As per corporate standard>
Message title for users attempting to log on		<As per corporate standard>
Number of previous logons to cache (in case domain controller is not available)	10 logons	0 logons
Prevent system maintenance of computer account password	Disabled	Not defined
Prevent users from installing printer drivers	Enabled	Enabled
Prompt user to change password before expiration	14 days	7 days
Recovery Console: Allow automatic administrative logon	Disabled	Disabled
Recovery Console: Allow floppy copy and access to all drives and all folders	Disabled	Disabled
Rename administrator account	Not defined	<Appropriate name> See guidance in Windows 2000 Server Security Standards
Rename guest account	Not defined	<Appropriate name> See guidance in Windows 2000 Server Security Standards
Restrict CD-ROM access to locally logged-on user only	Disabled	Enabled
Restrict floppy access to locally logged-on user only	Disabled	Enabled



Secure channel: Digitally encrypt or sign secure channel data (always)	Disabled	Disabled
Secure channel: Digitally encrypt secure channel data (when possible)	Enabled	Enabled
Secure channel: Digitally sign secure channel data (when possible)	Enabled	Enabled
Secure channel: Require strong (Windows 2000 or later) session key	Disabled	Disabled
Secure system partition (for RISC platforms only)	Not defined	Not defined
Send unencrypted password to connect to third-party SMB servers	Disabled	Disabled
Shut down system immediately if unable to log security audits	Disabled	Disabled
Smart card removal behavior	No Action	No Action
Strengthen default permissions of global system objects (e.g. Symbolic Links)	Enabled	Enabled
Unsigned driver installation behavior	Not defined	Warn but allow installation
Unsigned non-driver installation behavior	Not defined	Warn but allow installation

Domain Controller Event Log settings

- The event logs should be configured large enough to contain the data generated between backup cycles. For example, if log backups occur each week, ensure the logs are large enough to hold a week's worth of events. Once the appropriate size has been determined, select **Overwrite events older than...** at least the number of days between backups (Event Log\Settings for Event Logs).



Member/Stand-Alone Server Policies

Member/Stand-Alone Server Audit Policy

- Set the following Audit Policy in *Local Policies\Audit Policy*:

Policy	Default setting	Recommended setting
Audit account logon events	No auditing	Success, Failure
Audit account management	Not defined	Success, Failure
Audit directory service access	Not defined	No auditing
Audit logon events	No auditing	Success, Failure
Audit object access	No auditing	Failure
Audit policy change	No auditing	Success, Failure
Audit privilege use	No auditing	Failure
Audit process tracking	No auditing	No auditing
Audit system events	No auditing	Success, Failure

- Note that enabling auditing for object access does not in itself cause any auditing of objects. Rather it *enables the possibility* of object auditing, which then requires specific objects (e.g. files, folders) to have auditing enabled for specific users or groups in order to generate events in the Security Event Log.

User Rights Assignment

- Set the following User Rights Assignment in *Local Policies\User Rights Assignment*:

Policy	Default setting	Recommended setting
Access this computer from the network	Administrators, Backup Operators, Power Users, Users, Everyone	Administrators, Backup Operators, Power Users, Users
Act as part of the operating system		None
Add workstations to domain		None
Back up files and directories	Administrators, Backup Operators	Backup Operators
Bypass traverse checking	Administrators, Backup Operators, Power Users, Users, Everyone	Administrators (Users also required for IIS)

Windows 2000 Security Templates



Change the system time	Administrators, Power Users	Administrators
Create a pagefile	Administrators	Administrators
Create a token object		None
Create permanent shared objects		
Debug programs	Administrators	None
Deny access to this computer from the network		None
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	Administrators	Administrators
Generate security audits		
Increase quotas	Administrators	Administrators
Increase scheduling priority	Administrators	Administrators
Load and unload device drivers	Administrators	Administrators
Lock pages in memory		None
Log on as a batch job		
Log on as a service		None
Log on locally	Administrators, Backup Operators, Power Users, Users, Guest	Administrators, Backup Operators, Power Users
Manage auditing and security log	Administrators	Administrators
Modify firmware environment values	Administrators	Administrators
Profile single process	Administrators, Power Users	Administrators
Profile system performance	Administrators	Administrators
Remove computer from docking station	Administrators, Power Users, Users	Administrators
Replace a process level token		None
Restore files and directories	Administrators, Backup Operators	Backup Operators
Shut down the system	Administrators, Backup	Administrators

Windows 2000 Security Templates



	Operators, Power Users	
Synchronize directory service data		
Take ownership of files or other objects	Administrators	Administrators

- *None* means that no users or groups must be granted the privilege

Security Options

- Set the following Security Options in *Local Policies\Security Options*:

Policy	Default setting	Recommended setting
Additional restrictions for anonymous connections	None. Rely on default permissions	No access without explicit anonymous permissions
Allow server operators to schedule tasks (domain controllers only)	Not defined	Not defined
Allow system to be shut down without having to log on	Disabled	Disabled
Allowed to eject removable NTFS media	Administrators	Administrators
Amount of idle time required before disconnecting session	15 minutes	15 minutes
Audit the access of global system objects	Disabled	Enabled
Audit use of Backup and Restore privilege	Disabled	Enabled
Automatically log off users when logon time expires	Not defined	
Automatically log off users when logon time expires (local)	Enabled	Enabled
Clear virtual memory pagefile when system shuts down	Disabled	Enabled
Digitally sign client communication (always)	Disabled	Disabled
Digitally sign client communication (when possible)	Enabled	Enabled
Digitally sign server communication (always)	Disabled	Disabled

Windows 2000 Security Templates



Digitally sign server communication (when possible)	Disabled	Enabled
Disable CTRL+ALT+DEL requirement for logon	Disabled	Disabled
Do not display last user name in logon screen	Disabled	Enabled
LAN Manager Authentication Level	Send LM & NTLM responses	Send NTLM response only
Message text for users attempting to log on		<As per corporate standard>
Message title for users attempting to log on		<As per corporate standard>
Number of previous logons to cache (in case domain controller is not available)	10 logons	0 logons
Prevent system maintenance of computer account password	Disabled	Not defined
Prevent users from installing printer drivers	Enabled	Enabled
Prompt user to change password before expiration	14 days	7 days
Recovery Console: Allow automatic administrative logon	Disabled	Disabled
Recovery Console: Allow floppy copy and access to all drives and all folders	Disabled	Disabled
Rename administrator account	Not defined	<Appropriate name> See guidance in Windows 2000 Server Security Standards
Rename guest account	Not defined	<Appropriate name> See guidance in Windows 2000 Server Security Standards
Restrict CD-ROM access to locally logged-on user only	Disabled	Enabled
Restrict floppy access to locally logged-on user only	Disabled	Enabled
Secure channel: Digitally encrypt or sign secure channel data (always)	Disabled	Disabled
Secure channel: Digitally encrypt	Enabled	Enabled



secure channel data (when possible)		
Secure channel: Digitally sign secure channel data (when possible)	Enabled	Enabled
Secure channel: Require strong (Windows 2000 or later) session key	Disabled	Disabled
Send unencrypted password to connect to third-party SMB servers	Disabled	Disabled
Shut down system immediately if unable to log security audits	Disabled	Disabled
Smart card removal behavior	No Action	No Action
Strengthen default permissions of global system objects (e.g. Symbolic Links)	Enabled	Enabled
Unsigned driver installation behavior	Not defined	Warn but allow installation
Unsigned non-driver installation behavior	Not defined	Warn but allow installation

Event Log settings

- The event logs should be configured large enough to contain the data generated between backup cycles. For example, if log backups occur each week, ensure the logs are large enough to hold a week's worth of events. Once the appropriate size has been determined, select **Overwrite events older than...** at least the number of days between backups (Event Log\Settings for Event Logs).



Workstation Policies

Workstation Audit Policy

- Set the following Audit Policy in *Local Policies\Audit Policy*:

Policy	Default setting	Recommended setting
Audit account logon events	No auditing	No auditing
Audit account management	No auditing	No auditing
Audit directory service access	Not defined	Not defined
Audit logon events	No auditing	No auditing
Audit object access	No auditing	No auditing
Audit policy change	No auditing	No auditing
Audit privilege use	No auditing	No auditing
Audit process tracking	No auditing	No auditing
Audit system events	No auditing	No auditing

User Rights Assignment

- Set the following User Rights Assignment in *Local Policies\User Rights Assignment*:

Policy	Default setting	Recommended setting
Access this computer from the network	Administrators, Backup Operators, Power Users, Users, Everyone	None
Act as part of the operating system		None
Add workstations to domain		None
Back up files and directories	Administrators, Backup Operators	Backup Operators
Bypass traverse checking	Administrators, Backup Operators, Power Users, Users, Everyone	Administrators
Change the system time	Administrators, Power Users	Administrators
Create a pagefile	Administrators	Administrators
Create a token object		None
Create permanent shared objects		

Windows 2000 Security Templates



Debug programs	Administrators	None
Deny access to this computer from the network		None
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	Administrators	Administrators
Generate security audits		
Increase quotas	Administrators	Administrators
Increase scheduling priority	Administrators	Administrators
Load and unload device drivers	Administrators	Administrators
Lock pages in memory		None
Log on as a batch job		
Log on as a service		None
Log on locally	Administrators, Backup Operators, Power Users, Users, Guest	Administrators, Authenticated Users
Manage auditing and security log	Administrators	Administrators
Modify firmware environment values	Administrators	Administrators
Profile single process	Administrators, Power Users	Administrators
Profile system performance	Administrators	Administrators
Remove computer from docking station	Administrators, Power Users, Users	Administrators
Replace a process level token		None
Restore files and directories	Administrators, Backup Operators	Backup Operators
Shut down the system	Administrators, Backup Operators, Power Users, Users	Authenticated Users
Synchronize directory service data		
Take ownership of files or other objects	Administrators	Administrators



- *None* means that no users or groups must be granted the privilege

Security Options

- Set the following Security Options in *Local Policies\Security Options*:

Policy	Default setting	Recommended setting
Additional restrictions for anonymous connections	None. Rely on default permissions	No access without explicit anonymous permissions
Allow server operators to schedule tasks (domain controllers only)	Not defined	Not defined
Allow system to be shut down without having to log on	Enabled	Disabled
Allowed to eject removable NTFS media	Administrators	Administrators
Amount of idle time required before disconnecting session	15 minutes	15 minutes
Audit the access of global system objects	Disabled	Disabled
Audit use of Backup and Restore privilege	Disabled	Disabled
Automatically log off users when logon time expires	Not defined	Not defined
Automatically log off users when logon time expires (local)	Enabled	Enabled
Clear virtual memory pagefile when system shuts down	Disabled	Enabled
Digitally sign client communication (always)	Disabled	Disabled
Digitally sign client communication (when possible)	Enabled	Enabled
Digitally sign server communication (always)	Disabled	Disabled
Digitally sign server communication (when possible)	Disabled	Enabled
Disable CTRL+ALT+DEL requirement for logon	Not defined	Disabled
Do not display last user name in	Disabled	Enabled

Windows 2000 Security Templates



logon screen		
LAN Manager Authentication Level	Send LM & NTLM responses	Send NTLM response only
Message text for users attempting to log on		<As per corporate standard>
Message title for users attempting to log on		<As per corporate standard>
Number of previous logons to cache (in case domain controller is not available)	10 logons	0 logons
Prevent system maintenance of computer account password	Disabled	Not defined
Prevent users from installing printer drivers	Disabled	Enabled
Prompt user to change password before expiration	14 days	7 days
Recovery Console: Allow automatic administrative logon	Disabled	Disabled
Recovery Console: Allow floppy copy and access to all drives and all folders	Disabled	Disabled
Rename administrator account	Not defined	<Appropriate name> See guidance in Windows 2000 Professional Security Standards
Rename guest account	Not defined	<Appropriate name> See guidance in Windows 2000 Professional Security Standards
Restrict CD-ROM access to locally logged-on user only	Disabled	Enabled
Restrict floppy access to locally logged-on user only	Disabled	Enabled
Secure channel: Digitally encrypt or sign secure channel data (always)	Disabled	Disabled
Secure channel: Digitally encrypt secure channel data (when possible)	Enabled	Enabled
Secure channel: Digitally sign	Enabled	Enabled



secure channel data (when possible)		
Secure channel: Require strong (Windows 2000 or later) session key	Disabled	Disabled
Send unencrypted password to connect to third-party SMB servers	Disabled	Disabled
Shut down system immediately if unable to log security audits	Disabled	Disabled
Smart card removal behavior	No Action	No Action
Strengthen default permissions of global system objects (e.g. Symbolic Links)	Enabled	Enabled
Unsigned driver installation behavior	Not defined	Warn but allow installation
Unsigned non-driver installation behavior	Not defined	Warn but allow installation

Event Log settings

- The event logs should be configured large enough to contain the data generated between backup cycles. For example, if log backups occur each week, ensure the logs are large enough to hold a week's worth of events. Once the appropriate size has been determined, select **Overwrite events older than...** at least the number of days between backups (Event Log\Settings for Event Logs).



References

The following sources were used as reference material in the production of this document:

- *Microsoft Security Tool Kit* (Microsoft Corporation)
- *Security Operations Guide for Windows 2000 Server* (Microsoft Corporation)
- *Securing Windows 2000 Step by Step* (The SANS Institute)
- *Hardening Windows 2000* (SystemExperts Corporation)