



Introduction

This document specifies the organisation's security standards for computers running Microsoft Windows NT Server. It is intended to provide instructions for securing both existing systems and new installations, and is organised in two sections: mandatory standards and recommended good practice.

Mandatory standards are those that must be applied in all cases. Recommended good practice consists of additional guidance from First Base Technologies that is offered for serious consideration in order to strengthen existing security measures.

Where specific software tools are required to achieve certain of the recommendations (e.g. virus control), this document does not identify or describe those tools, since it is likely that they will change as time passes and the organisation discovers more appropriate methods of achieving the end result. Please refer to the appropriate documentation for the tool currently being used for each task.

These standards and recommendations should be thoroughly tested before implementation on live systems.



Mandatory standards

Physical & environmental security

- Locate servers in a secure room with access controlled by the administration team
- Change numeric access control codes every 90 days, whenever an authorised individual ceases to require access and whenever code compromise is suspected
- Ensure that uncontrolled access is not possible via suspended ceilings and raised floors
- Review server room access control lists every 6 months
- Place servers in secure racks and establish a procedure to ensure that keys are protected and yet easily available to appropriate authorised personnel. Ensure that backup keys are held off-site in a fireproof safe.
- Position system keyboards and screens so they are not overlooked by windows or other vantage points
- Ensure that servers are not left logged on when unattended, or where this is unavoidable (e.g. where a required application cannot be run as a service) that the console is secured using the “Lock Workstation” feature
- Ensure that all servers are protected by a UPS and associated software that allows automatic clean shut down
- Ensure that temperature and humidity controls are sufficient to comply with the manufacturers’ recommendations
- Ensure that sufficient fire extinguishers of an appropriate type are provided and that smoke alarms are fitted

Disabling unused hardware

- Remove or disable hardware devices (including serial and parallel ports, and unused removable media drives) that may be viewed as a security risk



Securing the boot sequence

- Configure servers to boot first from the hard disk, then from the diskette and/or CD-ROM
- On mission-critical servers, disable the diskette drive and CD-ROM in the BIOS (there is a registry setting to disable them under Windows NT, however this only disables them as network shares - they are still available to the local user and can still be used to boot the computer)

NTFS file system

- Ensure that all fixed disk partitions are formatted with NTFS
- Existing FAT volumes can be converted to NTFS without loss of data using the CONVERT utility
- Set NTFS permissions on converted system partitions to the default levels using the FIXACLS utility from the Windows NT4.0 Resource Kit
- Ensure that user data and application code are placed on separate NTFS partitions from operating system files to help ensure that users do not accidentally gain access to critical system files. In addition, if a user partition is entirely filled, the operating system and its paging file will be unaffected (Windows NT may crash if it runs out of available free drive space).

Removing unused subsystems

- After verifying that they are not required to run any essential application software, remove the OS/2 and POSIX subsystems by deleting the following strings from the registry:

Hive	HKEY_LOCAL_MACHINE
Key	System\CurrentControlSet\Control\Session Manager\Subsystems
Value Name	Optional
Strings	Os2, Posix

- Delete the following files from the \Winnt\System32 folder:



os2.exe
os2srv.exe
os2ss.exe
pax.exe
posix.exe
psxdll.dll
psxss.exe

Restricting remote access to the registry

- Locate and select the following registry key using REGEDT32.EXE:

Hive	HKEY_LOCAL_MACHINE
Key	\System\CurrentControlSet\Control\SecurePipeServers
Value Name	\winreg

- Select Permissions from the Security menu
- Ensure that SYSTEM and Administrators are granted Full Control and that no other users or groups are listed
- Specify applications that require remote registry access using non-administrative credentials under:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipesServer
\Winreg\AllowedPaths.

Restricting anonymous access to Local Security Authority information

This prevents anonymous users from enumerating users, groups, shares, etc.

- Set the following registry value (if it does not exist, then create it):

Hive	HKEY_LOCAL_MACHINE
Key	System\CurrentControlSet\Control\LSA
Value Name	RestrictAnonymous
Type	REG_DWORD
Value	1



Disabling LanMan authentication

- Set the following registry value (if it does not exist, then create it):

Hive	HKEY_LOCAL_MACHINE
Key	System\CurrentControlSet\Control\LSA
Value Name	LMCompatibilityLevel
Type	REG_DWORD
Value	2

Disabling cached logon information

- Set the following registry value (if it does not exist, then create it):

Hive	HKEY_LOCAL_MACHINE
Key	Software\Microsoft\Windows NT\CurrentVersion\Winlogon
Value Name	CachedLogonsCount
Type	REG_SZ
Value	0

Disabling the display of last logged on username

- Set the following registry value (if it does not exist, then create it):

Hive	HKEY_LOCAL_MACHINE
Key	Software\Microsoft\Windows NT\CurrentVersion\Winlogon
Value Name	DontDisplayLastUsername
Type	REG_SZ
Value	1

Configuring a logon warning banner

- Set the following registry values (if they do not exist, then create them):

Hive	HKEY_LOCAL_MACHINE
Key	Software\Microsoft\Windows NT\CurrentVersion\Winlogon
Value Name	LegalNoticeCaption
Type	REG_SZ
Value	<Standard organisation warning message header>



Hive	HKEY_LOCAL_MACHINE
Key	Software\Microsoft\Windows NT\CurrentVersion\Winlogon
Value Name	LegalNoticeText
Type	REG_SZ
Value	<Standard organisation warning message text>

Securing the registry

- Change the permissions for the *Everyone* group for the following registry entries to **Read**:

Key path	Prevents users from
\SOFTWARE	Installing software
\SOFTWARE\Microsoft\RPC	Gaining access to RPC configuration information
\SOFTWARE\Microsoft\WindowsNT\CurrentVersion	Gaining Windows NT version information
\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Perflib	Using the Performance Monitor to view the performance of the computer
\SYSTEM\CurrentControlSet\Services\Lanman Server\Shares	Changing share information
\SYSTEM\CurrentControlSet\Services\UPS	Accessing UPS configuration
HKEY_USERS\.DEFAULT	Changing the default user setting
HKEY_CLASSES_ROOT and all sub keys	Changing file associations and OLE configurations

Securing the file system

- Set file and directory ACLs as shown below:

Folder(s)	User/Group	Permissions
\Winnt and all subfolders	Administrators: SYSTEM: CREATOR OWNER: Users:	Full Control Full Control Full Control Read
\Winnt\Repair	Administrators:	Full Control
\Winnt\System32\config	Administrators: SYSTEM:	Full Control Full Control



	CREATOR OWNER: Users:	Full Control List
\\Winnt\System32\spool	Administrators: SYSTEM: CREATOR OWNER: Users:	Full Control Full Control Full Control Read
\\Winnt\Cookies \\Winnt\Forms \\Winnt\History \\Winnt\Temporary Internet Files \\Winnt\Profiles \\Winnt\SendTo \\Winnt\OcCache	Administrators: SYSTEM: CREATOR OWNER: Users:	Full Control Full Control Full Control Special Directory Access Read, Write & Execute Special File Access - None Specified
\\Temp	Administrators: SYSTEM: CREATOR OWNER: Users:	Full Control Full Control Full Control Special Directory Access Read, Write & Execute Special File Access - None Specified
C:\Boot.ini C:\Ntdetect.com C:\Ntldr	Administrators: SYSTEM: CREATOR OWNER:	Full Control Full Control Full Control
Root of all new partitions	Administrators: Server Operators:	Full Control Full Control

Securing the Administrator account

- Rename the Administrator account to a non-obvious name, in line with your standard account naming conventions
- For each domain, define a 14-character complex password¹ and assign it to the original Administrator account on each server in the domain
- Record the password and store it in a physically secure location to which only the Systems Security team have access

¹ Please see *Enforcing complex passwords* in the *Recommended good practice* section of this document



- Change the password(s) if an administrator who knows them leaves the organisation or is reassigned to a non-administrative role, or if you suspect the password(s) have been compromised.
- Create a “sacrificial goat” account named Administrator with no privileges and ensure that the event log is inspected regularly for evidence of attempts to use this account
- Enable account lockout across the network on the original Administrator account by using the PASSPROP.EXE utility from the Windows NT 4.0 Server Resource Kit

Establishing separate accounts for Administrators

- Create separate administrator-equivalent accounts for each individual who genuinely requires administrative privilege to perform elements of their job function (as few as is strictly necessary)

Securing the Guest account

- Ensure the account is disabled
- Rename the account to a non-obvious name, in line with your standard account naming conventions
- Set a complex 14-character password² on the account
- Restrict its Logon Hours to disallow logon at all times
- Restrict its Logon Workstations to one non-existent workstation name

Disabling unnecessary services

- Disable any services not required for the server to perform its role. In particular, consider whether the server needs any IIS components and whether it should be running the Server service for file and print sharing.
- Do not install any applications or utility software on the server unless they are strictly required for the server to perform its role

² Please see *Enforcing complex passwords* in the *Recommended good practice* section of this document



Configuring the Account Policy

- Set the following Account Policy:

Parameter	Setting
Maximum password Age	60 days
Minimum password Age	14 days
Minimum password length	6 characters
Password uniqueness	8
Account lockout after	3 bad logon attempts
Reset account after	30 Minutes
Lockout duration	Forever (until unlocked by Security Admin)
Forcibly disconnect remote users from server when logon hours expire	No
Users must logon in order to change password	No

Configuring the User Rights Policy

- Make the following changes on Primary and Backup Domain Controllers:

User Right	Groups assigned this right by default on domain controller	Change for domain controller
Access this computer from the network Allows a user to connect over the network to the computer	Administrators, Everyone	Administrators, Backup Operators, Server Operators, Print Operators, Users
Bypass traverse checking Allows a user to change directories and travel through a directory tree, even if the user has no permissions for those directories	Everyone	<none>
Log on locally Allows a user to log on at the computer, from the computer's keyboard	Account Operators, Administrators, Backup Operators, Server Operators, Print Operators	Administrators, Backup Operators, Server Operators
Shut down the system Allows a user to shut down	Account Operators, Administrators, Backup	Administrators, Backup Operators, Server Operators

Windows NT Server Security Standards



Windows NT	Operators, Server Operators, Print Operators	
------------	--	--

- Make the following changes on Member Servers:

User Right	Groups assigned this right by default on member server	Change for member server
Access this computer from the network Allows a user to connect over the network to the computer	Administrators, Everyone and Power Users	Administrators, Backup Operators, Users, Power Users
Bypass traverse checking Allows a user to change directories and travel through a directory tree, even if the user has no permissions for those directories	Everyone	<none>
Log on locally Allows a user to log on at the computer, from the computer's keyboard	Administrators, Backup Operators, Everyone, Guests, Power Users, and Users	Administrators, Backup Operators, Power Users
Shut down the system Allows a user to shut down Windows NT	Administrators, Everyone, Guests, Power Users, and Backup Operators	Administrators, Backup Operators, Power Users

Configuring the audit policy

- Set the following Audit Policy:

Audit Category	Recommended setting	Comments
Logon and Logoff	Success & Failure	Fundamental security requirement - to detect attempted break-in using random passwords, or actual break-in using a stolen password
File and Object Access	Failure only	Where appropriate – to detect improper access to sensitive files (requires additional configuration of file or folder audit properties)
Use of User Rights	Failure only	Fundamental security requirement - to detect attempted improper user activity



User & Group Management	Success & Failure	Fundamental security requirement
Security Policy Changes	Success & Failure	Fundamental security requirement
Restart, Shutdown & System	Success & Failure	Unless the volume of events generated by “System” proves to be overwhelming, in which case Failure only
Process Tracking	None	Specialist security requirement that produces a very large audit trail – not normally required for production environments

Configuring Event Log settings

- Configure the following log settings:

Log	Maximum Log Size	Event Log Wrapping
Application	2048 KB	Overwrite Events as Needed
Security	2048 KB	Overwrite Events as Needed
System	2048 KB	Overwrite Events as Needed

Protecting console access

- Configure the Logon Screen Saver to activate after 10 minutes of inactivity and to be password protected

Creating & securing Emergency Boot Disks

- Create an Emergency Boot Disk for each machine (or class of machine where the disk configuration is identical) and test that it can be used to boot the system
- Store the disks in an appropriate secure location, with access restricted to designated personnel
- Ensure that copies are held off-site in a fireproof safe
- Ensure that disks are updated if changes are made to a system’s disk configuration

Creating & securing Emergency Repair Disks

- Create an Emergency Repair Disk for each machine



- Store the disks in an appropriate secure location, with access restricted to designated personnel
- Ensure that disks are updated each time changes are made to a system's configuration
- Ensure that up-to-date copies are held off-site in a fireproof safe

Limiting trust relationships

- Ensure that only authorised trust relationships are configured (in particular ensure that no inappropriate trust relationships are left in place after test scenarios have been completed and the trusts are no longer required).

Securing Internet Explorer

- Ensure that Internet Explorer is required to be installed and remove it if not
- Where required, ensure that the latest approved version is installed
- Ensure that the latest approved Service Pack and post-SP hotfixes are applied (see below)

Securing Internet Information Server (if appropriate)

- Ensure that IIS is required to be installed and remove it if not
- Where required, ensure that the latest approved version is installed
- Run the IIS Lockdown Wizard from the Microsoft Security Tool Kit (included as part of the TechNet distribution) to configure IIS for secure operation
- Ensure that the latest approved Service Pack and post-SP hotfixes are applied (see below)

Installing anti-virus software and updates

- Ensure that the latest approved anti-virus product, appropriate to the machine's role, is installed and configured in line with organisation standards

Installing the latest (approved) service pack

- Ensure that the latest approved Service Pack is installed



- “approved” means that a formal test process has been carried out to ensure compatibility with all relevant system software and applications, meaning that given configurations could require different service packs

Installing the appropriate post-service pack security hotfixes

- Ensure that the latest approved post-SP hotfixes are applied as appropriate
- “approved” means that a formal test process has been carried out to ensure compatibility with all relevant system software and applications, meaning that given configurations could require different post-SP hotfixes



Recommended good practice

Configuring the Account Policy

- The following stronger account policy is recommended for the reasons described:

Parameter	Setting	Justification
Maximum password Age	60 days	No change
Minimum password Age	1 day	To allow passwords to be changed by the user if compromise is suspected, while still discouraging the “cycling” of passwords
Minimum password length	7 characters	7 & 14 character passwords are proven to be the most secure because of the way the encrypted hashes are stored by Windows NT
Password uniqueness	13	To discourage month-related passwords
Account lockout after	3 bad logon attempts	No change
Reset account after	30 minutes	No change
Lockout duration	Forever (until unlocked by security admin)	No change
Forcibly disconnect remote users from server when logon hours expire	Yes	To increase security without infringing upon users’ <i>authorised</i> logon periods (users who frequently encounter this restriction should apply to have their logon hours extended)
Users must logon in order to change password	No	No change

Enforcing complex passwords

- 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 as far as is possible. A combination of both approaches is recommended. The following methods of enforcement are recommended for consideration (it should be noted that either method is likely to result in some additional administrative overhead, at least in the early stages of implementation):



- **Either** use the PASSPROP.EXE utility from the Windows NT Server Resource Kit to force users to select complex passwords (i.e. a combination made up from *any two* of lower case, upper case, numeric and symbol characters)
- **Or** install PASSFILT.DLL to enforce a tougher password filter (i.e. that requires a combination made up from *any three* of lower case, upper case, numeric and symbol characters, and disallows passwords related to the user's name)

Securing user accounts

- Create users only in domains (i.e. not on workstations or Member Servers)
- Allocate a unique username to each user
- Define a convention for usernames to simplify account creation
- Enable the option “User must change password at next logon” when creating a new account
- Ensure that regular user accounts do not have their password set to “Password never expires” (this does not apply to service accounts)
- Ensure that regular user accounts do not have their password set to “User cannot change password” (this does not apply to service accounts)
- Restrict each user's allowed Logon Hours as appropriate
- Restrict each user's allowed Logon Workstations where possible and appropriate

Configuring Domain Operators membership

- Improve management of the system by adding relevant users to the Account Operators, Server Operators, Backup Operators, Print Operators and Power Users Local Groups, rather than granting them full administrative powers
- Use the forms provided in the document “NT / W2K Rights and Abilities” to determine privileged access requirements

Configuring group memberships

- Create appropriate Local and Global Groups to match corporate requirements



- Use a naming convention that identifies the group type
- Assign users to Global Groups only
- Grant privileges to Local Groups only
- Allocate appropriate Global Groups to Local Groups

Configuring shares and setting appropriate ACLs

- Assign folder permissions to appropriate user groups in line with corporate policy. The following general points should be considered:
 - Executable files should be set to **Read**
 - Access to data files should be limited to defined groups rather than **Everyone**
 - The maximum permission assignment should be **Change** rather than **Full Control**, unless the ability to alter security or take ownership is explicitly required
 - Access to particularly sensitive files should be denied to all but a particular group, i.e. excluding any of the Administrator or domain Operators groups



References

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

- *Microsoft Security Tool Kit* (Microsoft Corporation)
- *Windows NT Security Checklist* (ISF)
- *Windows NT Security Guidelines* (NSA Research)
- *Windows NT Security Step by Step* (The SANS Institute)