

## Windows 2003 Member Server hardening document.

### Member Server Policy Recommendations

This section details the policy settings for The Company's GDP Member Server. The following security policy settings are reviewed:

- Audit Policy;
- User Right Assignment;
- Event Log;
- System File and Registry Key Permissions.

#### Audit Policy

Auditing is the process of analysing gathered data for the purpose or intent of determining a possible problem, or in the security arena, an attack or exploit.

QinetiQ's strategy concerning auditing implements a strong policy on auditing systems. As mentioned in previous documents, a centralised strategy for audit information with automated analysis and alerting should be implemented.

Control Statement	Control Procedure	Control Implication
Audit account logon events	Success, failure	This audits each instance of a user logging on to or logging off from another computer, in which the computer recording the audit event is used to validate the account. This can be useful to identify potential intrusion attempts.
Audit account management	Success, failure	This setting determines whether to audit each event of account management on a computer. A user account or group is created, changed, or deleted. A user account is renamed, disabled, or enabled. A password is set or changed. It is critical to track who is altering account permissions, legitimately or not.
Audit directory service access	Success, failure	Audits the event of a user accessing an Active Directory(AD) service object that has its own system access control list (ACL) specified.

Control Statement	Control Procedure	Control Implication
Audit logon events	Success, failure	Audits each instance of a user logging on to, logging off from, or making a network connection to the computer recording the audit event. Useful for forensics purposes.
Audit object access	Success, failure	Audits the event of a user accessing an object that has its own system ACLs specified. The object also requires auditing settings to be enabled.
Audit policy change	Success, failure	<p>An audit entry is generated when a change to user rights assignment policies, audit policies, or trust policies is successful. This is useful information for accounting purposes and for post-incident forensics, as it enables administrators to determine which users successfully modified policies in the domain or on individual computers.</p> <p>Currently setting the Control Procedure to Failure will not provide any meaningful events, however this has been added for completeness as it is envisaged these events will be used in the future by Microsoft (therefore this setting could be set to just Success as currently defined by Microsoft).</p>
Audit privilege use	Failure	Audits each instance of a user exercising a user right. Failure generates an audit entry each time that a user right is exercised unsuccessfully.
Audit process tracking	No auditing	This setting determines whether to audit detailed tracking information for events such as programme activation, process exit, handle duplication, and indirect object access.
Audit system events	Success, failure	<p>Audits when a user restarts or shuts down a computer, or when an event occurs that affects either the system security or the security log.</p> <p>Failure events could be useful in diagnosing a problem, such as failure of the system to shutdown. The Microsoft guide currently only</p>

Control Statement	Control Procedure	Control Implication
		recommends Success.

### User Rights Assignment

User rights determine which users or groups have logon rights or privileges on a computer. An example of a logon right is the right to logon to a computer locally. An example of a privilege is the right to shut down the system. Both types of user rights are assigned by administrators to individual users or groups as part of the security settings for each computer.

#### Note:

Because of unique SIDS that exist between Guests, Support\_388945a0, and Guest, some hardening settings cannot be automated using the security templates. These settings must be included in the incremental security templates.

User Rights “not defined” means Administrators still have privileges for every right not defined.

Control Statement	Control Procedure	Control Implication
Access this computer from the network (senetworklogonright)	Authenticated users, administrators	Users who can connect from their computer to the network can access resources on that computer for which they have permission. Users requiring access to member servers resources should be authenticated.
Act as part of the operating system (setcbprivilege)	Null Value – revoke all security groups and accounts	This allows a process to assume the identity of any user and thus gain access to the resources that the user is authorised to access. When a service requires this privilege, configure the service to log on using the local system account, which has this privilege inherently.  By default this right does not have anything assigned to it. With legacy systems this may have been altered to to allow level authentication services to function. It is mandatory that all security groups and accounts are revoked.
Add workstations to Domain (semachineaccountprivilege)	Administrators	Allows the user to add a computer to a specific domain. Users with this right could add a computer to the domain configured in a way that violates corporate security policies.  By default this right does not have

Control Statement	Control Procedure	Control Implication
		anything assigned to it. With legacy systems this may have been altered to allow other users or groups to add workstations to a domain. It is mandatory that all security groups and accounts are revoked apart from the Administrators group.
Adjust memory quotas for a process (seincreasequotaprivilege)	Administrators; local service; network service	Allows a user to adjust the maximum memory available to a process. Could be used to launch a Denial of Service (DoS) attack against business-critical network applications.
Allow logon locally (seinteractivelogonright)	Power users; backup operators; administrators	Allows a user to start an interactive session on the computer and could be used to log on at the console of the computer. This does not affect terminal services permissions.
Allow logon through terminal services (seremoteinteractivelogonright)	Administrators	This security setting determines which users or groups have permission to log on as a terminal services client.
Back up files and directories (sebackupprivilege)	Not defined	This right determines which users can bypass file and directory, registry, and other persistent object permissions for the purposes of backing up the system. Restoring backup media to an alternative location without permission constitutes a security vulnerability. If deemed necessary relevant groups may need to be added for backup software to function correctly.
Bypass traverse checking (sechangenotifyprivilege)	Not defined	This user right determines which users can traverse directory trees, even though the user may not have permissions on the traversed directory. This privilege does not allow the user to list the contents of a directory, only to traverse directories. As long as file system ACLs are set appropriately, this does not pose a problem. However if there are major concerns regarding these lists, then the 'everyone' group can be removed.
Change the system time (sesystemtimeprivilege)	Administrators	The potential vulnerability here relates to incorrect file and event log time stamps being and authentication issues. The risk is

Control Statement	Control Procedure	Control Implication
		mitigated because the Windows time service synchronises clocks throughout the domain.
Create a pagefile (secreatepagefileprivilege)	Administrators	Users who can change the page file size could make it extremely small or move the file to a highly fragmented storage volume, which could lead to reduced system performance.
Create a token object (secreatetokenprivilege)	Null Value - do not assign this right to any users.	Allows a process to create a token, which it can then use to gain access to any local resources. A user with the ability to create or modify tokens can change the level of access for any currently logged on account. They could escalate their own privileges or create a DoS condition. Do not assign the create a token object right to any users. Processes that require this privilege should use the local system account, which already includes this privilege.
Create global objects (secreateglobalprivilege)	Not defined	Users that can create global objects could degrade the performance of processes running under other users' sessions. This could lead to application failure or data corruption. Restricting the 'create global objects' user privilege to members of the local administrators and service groups could mitigate the risk. However Microsoft set this by default on a default setup therefore this option does not need to be explicitly set (i.e not defined).
Create permanent shared objects (secreatepermanentprivilege)	Null Value - do not assign this right to any users.	Users with this privilege could expose sensitive data to the network by creating a new shared object. Do not assign this right to any users. Processes that require this privilege should use the local system account, which already includes this privilege.
Debug programs (sedebbugprivilege)	Null Value - revoke all security groups and accounts.	The debug privilege can be exploited to capture sensitive system information from the system memory. Some attack tools exploit the debug programme's user right to extract hashed passwords and other private

Control Statement	Control Procedure	Control Implication
		security information. The risk of attackers being able to exploit this vulnerability is mitigated by the fact that the debug programme's user right is assigned only to administrators by default.
Deny access to this computer from the network (sedenetworklogonright)	<p>Anonymous logon; built-in administrator, guests; support_388945a0; guest; all non-operating system service accounts</p> <p>NB: Built-in Admin, Support_388945a0; Guest; and all NON operating system service accounts are not included in the security template. These groups and accounts have unique SIDS for each domain – therefore they must be added manually.</p>	<p>Users who can log onto the computer over the network can enumerate lists of account names, group names, and shared resources. Users with permission to access shared folders and files can connect over the network and possibly view or modify data. Explicitly denying this logon right to high-risk accounts, such as the local guest account and other accounts that have no business reason for accessing the computer over the network, provides an additional layer of protection.</p> <p>N.B.: an important exception to this list is any service account that is used to launch services that need to connect to the computer over the network. For example, if a shared folder for web servers to access and present content within that folder through a web site has been configured, it may be necessary to grant access to the account under which the Microsoft Internet Information Server (IIS) is running to allow it to log onto the server with the shared folder via the network.</p>
Deny logon as a batch job (sedenybatchlogonright)	<p>Guests; support_388945a0; guest</p> <p>NB: Support_xxxxxxx and guest are not included in the security template.</p>	Accounts with this logon right could be used to schedule jobs that could consume excessive system resources, leading to a DoS condition.
Deny logon as a service (sedenybatchlogonright)	<p>Not defined</p> <p>NB: ANONYMOUS LOGON, Built-in Admin, Support_388945a0; Guest; and all NON operating system service accounts are not included in the security template. These groups and</p>	Accounts that can log on as a service could be used to configure and launch new unauthorised services, such as a trojan horse or backdoor. The benefit of configuring this countermeasure is somewhat mitigated by the fact that only users with administrative privileges can install and configure

Control Statement	Control Procedure	Control Implication
	accounts have unique SIDS for each domain – therefore they must be added manually.	services, and an attacker who has already attained that level of access could configure the service to run with the local system account.
Deny logon locally (sedenyinteractivelogonright)	Not defined	Any account with the ability to log on locally could be used to log on at the console of the computer. Altering this right could limit the abilities of users assigned to specific administrative roles.
Deny log on through terminal services (sedenyremoteinteractivelogonright)	Built-in administrator; guests; support_388945a0; guest; all non-operating system service accounts  NB: ANONYMOUS LOGON, Built-in Admin, Support_388945a0; Guest; and all NON operating system service accounts are not included in the security template. These groups and accounts have unique SIDS for each domain – therefore they must be added manually.	Any account with the right to log on via terminal services could be used to log on to the remote console of the computer.
Enable computer and user accounts to be trusted for delegation (seenabledlegationprivilege)	There is no reason to assign this privilege to any user on member servers and workstations that belong to a domain because it has no meaning in those contexts; it is only relevant on DCs and stand-alone systems. Therefore this should be set to a Null Value – revoke all security groups and accounts.	Misuse of this privilege could lead to unauthorised users impersonating other users on the network. An attacker could exploit this privilege to gain access to network resources while appearing to be a different user, which could make it much more difficult to determine what has happened following a security incident.
Force shutdown from a remote system (seremotesutdownprivilege)	Administrators	Any user who can shut down a computer can cause a DoS condition; therefore, this privilege should be tightly restricted.
Generate security audits (seauditprivilege)	Local service; Network service	Accounts that are able to write to the security log could be used by an attacker to fill that log with meaningless events. If the computer is configured to overwrite events as needed, the attacker could use this method to remove evidence of their unauthorised activities. If the computer is configured to shut

Control Statement	Control Procedure	Control Implication
		down when it is unable to write to the security log, this method could be used to create a DoS condition.
Impersonate a client after authentication (seimpersonateprivilege)	Local service; network service	A user with this privilege could trick a client into connecting to a service that they have created and then impersonating that client. The user could then elevate their level of access to that of the other client.
Increase scheduling priority (seincreasebasepriorityprivilege)	Administrators	A user with this privilege could increase the scheduling priority of a process to real time. This would leave little processing time for all other processes, which could lead to a DoS condition.
Load and unload device drivers (seloaddriverprivilege)	Administrators	Device drivers run as highly privileged code. A user who has the load and unload device drivers privilege could unintentionally install malicious code masquerading as a device driver. It is assumed that administrators will exercise greater care and install only drivers with verified digital signatures.
Lock pages in memory (selockmemoryprivilege)	Administrators	Users with this privilege could assign physical memory to several processes, leaving little or no random access memory (RAM) for other processes. This could lead to a DoS condition.
Log on as a batch job (sebatchlogonright)	Null Value – revoke all security groups and accounts.	Allows a process to keep data in physical memory, which prevents the system from paging the data to virtual memory on disk. Enabling this user right can result in significant degradation of system performance. Users with this privilege can assign physical memory to several processes, leaving little or no RAM for other processes.
Log on as a service (seservicelogonright)	Not defined	This is a powerful logon right, which allows accounts to launch network services. The risk is mitigated by the fact that only users with administrative privileges can install and configure services. An attacker who has already attained that level of access could configure the service to run with the local system account.

Control Statement	Control Procedure	Control Implication
Manage auditing and security log (sesecurityprivilege)	Administrators	The right to manage the security event log is a powerful user privilege and it should be closely guarded. Anyone with this privilege can clear the security log, possibly erasing important evidence of unauthorised activity.
Modify firmware environment values (sesystemenvironmentprivilege)	Administrators	Anyone with this privilege could configure the settings of a hardware component, in such a way as to cause it to fail.
Perform volume maintenance tasks (semanagevolumeprivilege)	Administrators	A user with this privilege could delete a volume, leading to the loss of data or a DoS condition.
Profile single process (seprofilesingleprocessprivilege)	Administrators	An attacker with this privilege could monitor a computer's performance to help identify critical processes that they might wish to attack directly. The attacker may also be able to determine what processes are running on the system, thus allowing them to identify countermeasures that they may need to avoid, such as anti-virus software or an intrusion detection system (IDS).
Profile system performance (sesystemprofileprivilege)	Administrators	An attacker with this privilege could monitor a computer's performance to help identify critical processes that they might wish to attack directly. The attacker may also be able to determine what processes are running on the system, thus allowing them to identify countermeasures that they may need to avoid, such as anti-virus software or an intrusion detection system (IDS).
Remove computer from docking station (seundockprivilege)	Administrators	Allows the user of a laptop computer to undock the computer by clicking 'Eject PC' on the start menu.
Replace a process level token (seassignprimarytokenprivilege)	Local service; network service	A user with this privilege and the right to increase quotas for processes – the 'adjust memory quotas for a process' right – is able to launch processes as if they were another user. They could use this method to hide the fact that they are performing unauthorised

Control Statement	Control Procedure	Control Implication
		actions on the computer.
Restore files and directories (serestoreprivilege)	Administrators	An attacker with this privilege could restore sensitive corporate data to a system, overwriting data that is more recent. This could lead to loss of important data or data corruption. Note: this countermeasure will not prevent an attacker from restoring the data to an unmanaged system, so it is critical that organisations carefully protect the media used for backing up data.
Shut down the system (seshutdownprivilege)	Administrators	The ability to shut down a server should be limited to a very small number of trusted administrators. Even though a system shutdown requires the ability to log on to the server, care needs to be taken to prevent the obvious DoS implications.
Synchronise directory service data (sesynchagentprivilege)	Null Value – Revoke all security groups and accounts.	Only DCs should be able to synchronise directory service data.
Take ownership of files or other objects (setakeownershipprivilege)	Administrators	Any user with this ability can take control of any object, regardless of the permissions on that object, and then make any changes to it they wish. This could result in exposure or corruption of data.

## Security Options

Security options enable or disable computer security settings, such as digital data signing, administrator and guest account names, access to floppy disk and CD-ROM drives, driver installation behaviour and logon prompts.

Control Statement	Control Procedure	Control Implication
<b>Accounts</b>		
Guest account status	Disabled	This account allows unauthenticated network users to gain access to the system by logging in as 'guest' with no password. Unauthorised users could access any resources that are accessible to the guest account over the network. This means that any network shares with permissions allowing access to the guest account, the guests group, or the

Control Statement	Control Procedure	Control Implication
		everyone group will be accessible over the network. This could lead to the exposure or corruption of data.
Limit local account use of blank passwords to console logon only	Enabled	Blank passwords are a serious threat to computer security and they should be forbidden, through both corporate policy and suitable technical measures. Default settings for AD Domains require complex passwords of at least seven characters. Nevertheless, if a user with the ability to create new accounts makes one that has bypassed domain-based password policies, that account could have a blank password.
Rename administrator account	Not defined	Renaming the account makes it slightly more difficult for unauthorised persons to guess this privileged username and password combination. This is not defined as it may be that The Company's set this for all member servers via a GP or on an individual basis. Either way it is mandatory that the Administrator account is renamed.
Rename guest account	Not defined	Renaming the guest account makes it slightly more difficult for unauthorised persons to guess this privileged username and password combination. This is not defined as it may be The Company's set this for all member servers via a GP or on an individual basis. Either way it is amandatory that the Administrator account is renamed.
<b>DCOM</b>		
Machine Access Restrictions in Security Descriptor Language (SDDL) Syntax	Everyone: LC, RC Anonymous: LC, RC  Where: LC=Local Access Calls and RC=Remote Access Calls.	This is a new setting in Windows 2003 SP1. The values shown here (which are the default settings) will not cause any backwards compatibility issues for existing DCOM based applications.
Machine Launch Restrictions in Security Descriptor Language (SDDL) Syntax	Administrator: LL, LA, RL, RA Everyone: LL, LA Distributed COM users: LL, LA, RL, RA  Where: LL=Local Launch, LA=Local Activation, RL=Remote Launch and RA=Remote Activation.	This is a new setting in Windows 2003 SP1. The values shown here (which are the default settings) should not cause problems for existing DCOM applications. The settings prevent all but administrators and members of the Distributed COM users group from

Control Statement	Control Procedure	Control Implication
		remotely launching DCOM services. If an existing DCOM application does require a non-administrative user to start the service, the user should be added to the Distributed COM users group. Note that once the DCOM application has been launched, normal users can access it as before due to the Machine Access Restrictions setting above.
<b>Audit</b>		
Audit the access of global system objects	Disabled	A globally visible named object, if incorrectly secured, could be acted upon by a malicious programme that knows the name of the object. For instance, if a synchronisation object such as a mutex had a poorly chosen discretionary ACLs, then a malicious program could access that mutex by name and cause the program which created it to malfunction. However, the risk of this occurring is very low.
Audit the use of backup and restore privilege	Disabled	Enabling this option when the 'audit privilege use' setting is also enabled generates an audit event for every file that is backed up or restored. This could help track down an administrator who is accidentally or maliciously restoring data in an unauthorised manner. Enabling this setting could generate a large number of security events, which could cause servers to respond slowly and force the security event log to record numerous events of little significance.
Shut down system immediately if unable to log security audits	Enabled	<p>If the computer is unable to record events to the security log, then critical evidence or important troubleshooting information may not be available for review after a security incident.</p> <p>Setting this to enabled can cause issues and does present a possible means to instigate a DOS attack. The Company's therefore need to determine whether keeping the service active is of a higher priority than recording security events.</p>

Control Statement	Control Procedure	Control Implication
		It is imperative that this option is reviewed and thoroughly tested as it could have serious implications on service availability
<b>Devices</b>		
Allow undock without having to log on	Disabled	Enabling this setting means that anyone with physical access to computers placed in their docking station could remove the computer and possibly tamper with it.
Allowed to format and eject removable media	Administrators	Users may be able to move removable disks to a different computer where they have administrative privileges. The user could then take ownership of any file, grant himself or herself full control and view or modify any file. The advantage of this setting is diminished by the fact that most removable storage devices will eject media with the press of a button.
Prevent users from installing printer drivers	Enabled	While it may be appropriate in some organisations to allow users to install printer drivers on their own workstations, this is not suitable for servers. Installing a printer driver on a server may unintentionally cause the system to become less stable. Only administrators should have this privilege on servers. A malicious user may deliberately try to damage the system by installing inappropriate printer drivers.
Restrict CD-ROM access to locally logged-on user only	Enabled	The benefit of this countermeasure is small because it only prevents network users from accessing the drive when someone is logged onto the local console of the system at the same time. Additionally, as CD-ROM drives are not automatically made available as network shares, administrators must deliberately choose to share the drive. This will be important when administrators are installing software or copying data from a CD-ROM that they do not want network users to be able to view.
Restrict floppy access	Enabled	The benefit of this countermeasure

Control Statement	Control Procedure	Control Implication
to locally logged-on user only		is small because it only prevents network users from accessing the drive when someone is logged onto the local console of the system at the same time. Additionally, as floppy drives are not automatically made available as network shares, administrators must deliberately choose to share the drive. This will be important when administrators are installing software or copying data from a floppy that they do not want network users to be able to view.
Unsigned driver installation behaviour	Warn but allow installation	<p>This option prevents the installation of unsigned drivers, or warns the administrator that unsigned driver software is about to be installed. This can prevent the installation of drivers via the Setup API that have not been certified to run on Windows Server 2003.</p> <p>This setting will not prevent a method used by some attack tools, where malicious .sys files are copied and registered to start as system services.</p> <p>It is imperative that this option is reviewed and thoroughly tested as it could impact the automated build process.</p>
<b>Domain Controller</b>		
Allow server operators to schedule tasks	Disabled	Enabling this setting means that jobs created by server operators via the "at" service will execute in the context of the account that is running that service. By default, this is the local system account. The impact of disabling this control should be small. This means that server operators could perform tasks that system is able to do but they are not, such as adding their account to the local administrators group.
LDAP server signing requirements	Require signing	Unsigned network traffic is susceptible to man-in-the-middle attacks, whereby an intruder captures packets between the server and the client and modifies

Control Statement	Control Procedure	Control Implication
		<p>them before forwarding them to the client. In the case of an LDAP server, this means that an attacker could cause a client to make decisions based on false records from the LDAP directory. The risk of an attacker successfully launching this attack in a corporate network can be mitigated by implementing strong physical security measures to protect the network infrastructure.</p> <p>Furthermore, implementing IPSec authentication header (AH) mode, which performs mutual authentication and packet integrity for Internet protocol (IP) traffic, can make all types of man-in-the-middle attacks extremely difficult.</p> <p>This setting will cause issues with domain controllers that are not running Windows 2000 or 2003 operating systems, such as Windows NT 4.0.</p>
Refuse machine account password changes	Disabled	Enabling this setting on all DCs in a domain prevents domain members from changing their computer account passwords. This in turn leaves those passwords susceptible to attack.
<b>Domain member</b>		
Digitally encrypt or sign secure channel data (always)	Enabled	After joining the domain, a computer uses the password for that account to create a secure channel with the DC for its domain every time that it restarts. Requests sent on the secure channel are
Digitally encrypt secure channel data (when possible)	Enabled	

Control Statement	Control Procedure	Control Implication
Digitally sign secure channel data (when possible)	Enabled	<p>authenticated and sensitive information such as passwords are encrypted, but the channel is not integrity checked, and not all information is encrypted. If a system is set to always encrypt or sign secure channel data, then a secure channel can not be established with a DC that is not capable of signing or encrypting all secure channel traffic, because all secure channel data is signed and encrypted. If the computer is configured to encrypt or sign secure channel data when possible, a secure channel can be established, but the level of encryption and signing is negotiated.</p> <p>To take advantage of these settings on member server, workstations and domain controllers all domain controllers in the relevant domain must be running Windows NT 4 with Service Pack 6a or later.</p>
Disable machine account password changes	Disabled	<p>The default configuration for computers running Windows Server 2003 that belong to a domain is that they are automatically required to change the passwords for their accounts every thirty days. Disabling this feature causes computers running Windows Server 2003 to retain the same passwords as their computer accounts. Computers that are no longer able to automatically change their account password are at risk should an attacker determine the password for the system's domain account.</p>
Maximum machine account password age	30 days	<p>In AD-based domains, each computer has an account and password, just like every user. By default, the domain members automatically change their domain password every thirty days. Increasing this interval significantly, or setting it to 0 so that the computers no longer change their passwords, gives an</p>

Control Statement	Control Procedure	Control Implication
		attacker more time to undertake a brute-force password guessing attack against one of the computer accounts.
Require strong (Windows 2000 or later) session key	Enabled	<p>Stronger session keys should always be used to help protect secure channel communications from eavesdropping and session hijacking network attacks. Eavesdropping is a form of hacking in which network data is read or altered in transit. The data can be modified to hide or change the sender, or to redirect it.</p> <p>N.B.: This will affect interoperability with legacy Microsoft operating systems, for instance you will be unable to join computers running Windows 2000 with this setting enabled to Windows NT 4.0 domains.</p>
<b>Interactive logon</b>		
Do not display last user name	Enabled	An attacker with access to the console or who is able to connect to the server via terminal services could view the name of the last user who logged on to the server. The attacker could then attempt to log on to the server by guessing the password, using a dictionary-based or brute-force attack.
Do not require CTRL+ALT+DEL	Disabled	Not having to press the CTRL+ALT+DEL key combination leaves users susceptible to attacks that attempt to intercept their passwords. Requiring that CTRL+ALT+DEL be pressed before users log on ensures that users are communicating by means of a trusted path when entering their passwords. An attacker could install a trojan horse program that looked like the standard Windows logon dialogue box and captures the user's password. The attacker would then be able to log on to the compromised account with whatever level of privilege that user has.

Control Statement	Control Procedure	Control Implication
Message text for users attempting to log on	You Will Commit A Criminal Offence If You Act Outside Your Authority In Relation To This Computer. The Penalty Is A Fine, Imprisonment, Or Both. If You Are Acting Outside Your Authority, Do Not Proceed Any Further. Please note that your use of this system may be monitored for Operational or Business reasons.	Not utilising this warning message setting leaves The Company's organisation legally vulnerable to trespassers who unlawfully penetrate the network.
Message title for users attempting to log on	Warning – Computer Misuse Act 1990	
Number of previous logons to cache (in case DC is not available)	0 logons	Users who access the server console will have their logon credentials cached on that server. An attacker who is able to access the file system of the server could locate this cached information and use a brute-force attack to determine user passwords. Windows mitigates this type of attack by encrypting the information; however, it is recommended that this be set to 0.
Prompt user to change password before expiration	14 days	It is mandatory that user passwords be configured to expire periodically. Users will need to be warned that their passwords are going to expire, or they may inadvertently become locked out of the system.
Require DC authentication to unlock workstation	Enabled	When cached credentials are used, any changes that have recently been made to the account – such as user rights assignments, account lockout, or the account being disabled – are not considered or applied.
Require smart card	Not defined – this will be required for the Branch Infrastructure.	<p>In an ideal situation this would be enabled; however, all users would have to use smart cards to log onto the network, which means that The Company's would have to have a reliable Public Key Infrastructure (PKI) in place, with smart cards, and smart card readers for all users.</p> <p>This setting will be required for the Branch infrastructure and therefore may require an additional incremental security template being applied etc.</p>

Control Statement	Control Procedure	Control Implication
Smart card removal behaviour	Lock workstation	If smart cards are used for authentication, then the computer should automatically lock itself when the card is removed to prevent unauthorised access. If smart cards are not present then this setting will be ignored, therefore it can be left as Lock workstation.
<b>Microsoft network client</b>		
Digitally sign communications (always)	Enabled	Using a method known as session hijacking, attackers can potentially intercept and modify unsigned Server Message Block (SMB) packets then modify the traffic and forward it to make the server perform undesirable actions. Alternatively, the attacker could pose as the server or client after a legitimate authentication and gain unauthorised access to data.  In mixed environments enabling the Digitally sign communications (always) statement will stop legacy clients from authenticating or gaining access to domain controllers. Windows 2000 or later supports digitally signing communications.
Digitally sign communications (if server agrees)	Enabled	
Send unencrypted password to third-party SMB servers	Disabled	Enabling this setting allows the server to transmit passwords in plain text across the network to other systems offering SMB services like Samba.
<b>Microsoft network server</b>		
Amount of idle time required before suspending session	15 minutes	Each SMB session consumes server resources. Establishing numerous null sessions will slow or possibly crash the server. An attacker could repeatedly establish SMB sessions until the server stops responding. SMB services will become slow or unresponsive.
Digitally sign communications (always)	Enabled	Using a method known as session hijacking, attackers can potentially intercept and modify unsigned SMB

Control Statement	Control Procedure	Control Implication
Digitally sign communications (if client agrees)	Enabled	<p>packets, then modify the traffic and forward it to make the server perform undesirable actions. Alternatively, the attacker could pose as the server or client after a legitimate authentication and gain unauthorised access to data.</p> <p>Only Windows 2000 Server, Windows 2000 Professional, Windows 2003 Server and Windows XP Professional currently include versions of SMB that support mutual authentication.</p>
Disconnect clients when logon hours expire	Enabled	<p>Determines whether to disconnect users who are connected to the local computer outside their user account's valid logon hours. This setting affects the SMB component. When this policy is enabled, it causes client sessions with the SMB service to be forcibly disconnected when the client's logon hours expire.</p>
<b>Network access</b>		
Allow anonymous sid/name translation	Not defined	<p>This security setting determines whether an anonymous user can request security identifier attributes for another user. If enabled, a user with knowledge of an administrator's SID could contact a computer that has this policy enabled and use the SID to get the administrator's name.</p> <p>N.B.: It is the recommended setting, this is disabled. As being disabled is the default setting on member servers there will have no impact on them and therefore is left as Not Defined. The default setting for DCs is enabled; this will be enforced by the DCs policy. It is important to remember that disabling this policy means that legacy systems may be unable to communicate with Windows Server 2003-based domains.</p>
Do not allow anonymous enumeration of SAM accounts	Enabled	<p>An unauthorised user could anonymously list account names and use the information to attempt to guess passwords or perform</p>

Control Statement	Control Procedure	Control Implication
Do not allow anonymous enumeration of sam accounts and shares	Enabled	social engineering attacks.
Do not allow storage of credentials or .Net passports for network authentication	Enabled	As passwords are cached a user may unknowingly execute hostile code that reads the passwords and forwards them to another, unauthorised user.
Let 'everyone' permissions apply to anonymous users	Disabled	This determines what additional permissions are granted for anonymous connections to the computer. Enabling this setting would allow anonymous users to perform certain activities, <b>for example: enumerating the names of domain accounts and network shares.</b> It should therefore be disabled.
Named pipes that can be accessed anonymously	Null value – setting enabled but no named pipes entered.	This security setting determines which communication sessions (pipes) will have attributes and permissions that allow anonymous access. Restricting access over named pipes such as comnap and locator helps prevent unauthorised access to the network.  <b>NB: If you need to enable this setting, ensure that you only add the named pipes that are needed to support the applications in your environment. This setting needs to be carefully tested before being deployed.</b>
Remotely accessible registry paths	System\currentcontrolset\control\prod ucoptions system\currentcontrolset\control\serv er applications software\Microsoft\Windows nt\currentversion  NB: Even is this security option is set, you must also start the Remote Registry system service if authorised users are going to be able to access the registry over the network.	An attacker could use this to facilitate unauthorised activities. To reduce the risk of this happening, suitable ACLs are assigned throughout the registry to help protect it from access by unauthorised users.

Control Statement	Control Procedure	Control Implication
Remotely accessible registry paths and subpaths	Software\Microsoft\Windows nt\currentversion\print software\Microsoft\Windows nt\currentversion\Windows system\currentcontrolset\control\print \printers system\currentcontrolset\services\eventlog software\Microsoft\olap server system\currentcontrolset\control\contentindex system\currentcontrolset\control\terminal server system\currentcontrolset\control\terminal server\userconfig system\currentcontrolset\control\terminal server\defaultuserconfiguration software\Microsoft\Windows nt\currentversion\perflib system\currentcontrolset\services\sysmonlog	
Restrict anonymous access to named pipes and shares	Enabled	Null sessions are a weakness that can be exploited through the various available shares.
Shares that can be accessed anonymously	Null Value – set to 'None'.	Enabling this setting is very dangerous. Any shares listed can be accessed by any network user. This could lead to the exposure or corruption of sensitive data.
Sharing and security model for local accounts	Classic - local users authenticate as themselves.	Determines how network logons that use local accounts are authenticated. If this setting is set to 'classic', network logons that use local account credentials authenticate by using those credentials. If this setting is set to guest only, network logons that use local accounts are automatically mapped to the guest account N.B.: this setting does not affect network logons that use domain accounts, nor does it affect interactive accounts.
<b>Network security</b>		
Do not store LAN manager hash value on next password change	Enabled	By attacking the SAM file, attackers can potentially gain access to usernames and passwords hashes. Enabling this setting will not prevent these types of attacks, but they will be much more difficult.  NB: Legacy OS and some third

Control Statement	Control Procedure	Control Implication
		party applications may fail when this setting is enabled. You also need to change the password on all accounts after enabling this setting.
Force logoff when logon hours expire	Not defined	If this setting is disabled, a user could remain connected to the system outside of their allotted logon hours. This is enforced at the domain policy level.
LAN manager authentication level	Send NTLMv2 responses only/refuse LM & NTLM	<p>This security setting determines which challenge/response authentication protocol is used for network logons. This choice affects the level of authentication protocol used by clients, the level of session security negotiated, and the level of authentication accepted by servers. This level of authentication is strongly recommended by QinetiQ and Microsoft. However, clients that do not support NTLMv2 authentication will not be able to authenticate in the Domain or access domain resources using LM and NTLM.</p> <p>NB: In a pure Windows NT4.0 SP4 or later environment – including Windows 2000 and XP – configure this setting to Send NTLMv2 responses only/refuse LM &amp; NTLM on all clients and then to Send NTLMv2 responses only/refuse LM &amp; NTLM on all servers. The exception to this is for the Windows 2003 RRAS server which will not function properly so consider setting to Send NTLMv2 responses only/refuse LM.</p>
LDAP client signing requirements	Negotiate signing	Unsigned network traffic is susceptible to man-in-the-middle attacks; this means that an attacker could cause a server to make decisions based on false queries from the LDAP client.
Minimum session security for NTLM SSP-based (including secure RPC) clients	Require message integrity, message confidentiality NTLMv2 session security and 128-bit encryption	This allows a client/server to require the negotiation of message confidentiality (encryption), message integrity, 128-bit

Control Statement	Control Procedure	Control Implication
Minimum session security for NTLM SSP-based (including secure RPC) servers	Require message integrity, message confidentiality, NTLMv2 session security and 128-bit encryption	encryption, or NTLMv2 session security. These values are dependent on the LAN manager authentication-level security setting value. These settings help to protect against man-in-the-middle attacks.
<b>Recovery console</b>		
Allow automatic administrative logon	Disabled	The recovery console can be very useful when troubleshooting and repairing systems that cannot be restarted. However, configuring this setting to enable automatic log on to the console is dangerous. This would allow anyone with physical access to the server, shut it down by disconnecting the power, reboot it, select Recover Console from the Restart menu and then assume full control of the server.
Allow floppy copy and access to all drives and all folders	Enabled	A potential vulnerability exists concerning using media at boot time to alter recovery console settings. In an ideal situation, this setting would be disabled. However, this would prevent legitimate use of the recovery console. Therefore, it is recommended that this setting be enabled, with other security methods put in place, such as physical security and, by default, disabling boot time access to floppy and CD-ROM drives.
<b>Shutdown</b>		
Allow system to be shut down without having to log on	Disabled	Users who can access the console locally could shut the system down. Therefore this should be disabled.
Clear virtual memory pagefile	Enabled	<p>An attacker who has physical access to a server that has been shut down could view the contents of the paging file. The attacker would move the system volume into a different computer and then analyse the contents of the paging file.</p> <p>This setting can cause sever delay when a system shuts down or is rebooted whcih can impact service availability. It is recommended testing is conducted to determine</p>

Control Statement	Control Procedure	Control Implication
		the delay. If the delay is not acceptable then this setting could be set to disabled but the highlighted risk must be managed.
<b>System cryptography</b>		
Force strong key protection for user keys stored on the computer	User must enter a password each time they use a key	This determines whether users' private keys, such as their s-Mime keys; require a password to be used. Enforcing password use every time a key is used means then even if an attacker takes control of a computer and determines what a user's logon password is, accessing locally stored user keys will be more difficult. N.B.: if the user overheads are deemed to become too great, then the value may be altered to prompt the user when the key is first used.
Use FIPS compliant algorithms for encryption, hashing, and signing	Disabled	In effect, this means that the provider only supports the Transport Layer Security (TLS) protocol as a client and as a server.  As this can serverly impact application and clients access this setting is currently not enabled. However, it is recommended that detailed testing be conducted to determine if it is feasible for FIPS compliant algorithms to be used. If it is feasible then the Control Procedure should be altered to enabled.
<b>System objects</b>		
Default owner for objects created by members of the administrators group	Object creator	This determines whether the administrators group or an object creator is the default owner of any system objects that are created.
Require case insensitivity for non-Windows subsystems	Enabled	All subsystems will be forced to observe case insensitivity.
Strengthen default permissions of internal system objects (e.g. symbolic links)	Enabled	Enabling this setting strengthens the default DACL, allowing non-administrator users to read shared objects, but not to modify shared objects that they did not create.
<b>System settings</b>		
Optional subsystems	Null value.	The POSIX subsystem introduces a security risk relating to processes that can persist across logins.

Control Statement	Control Procedure	Control Implication
Use certificate rules on Windows executables for software restriction policies	Not defined	This determines whether digital certificates are processed when a user or process attempts to run software with an .exe file name extension. Software Restriction Policies (SRP) help to protect users and computers from executing unauthorised code such as viruses and trojan horses. If SRP is used then the Control Procedure must be defined. See the QineitQ Overview for more information on SRP.

Table 5-3: Security option settings

### Event Log

Event Log reports contain information that can be useful in diagnosing problems and security related events. The Event Log service writes events sent by applications, services, and the operating system to log files. The events contain diagnostic information in addition to errors specific to the source application, service, or component. The following Event Log policy settings are recommended:

Control Statement	Control Procedure	Control Implication
Maximum application log size	16,386kb (Increase as necessary - see Control Implication)	Requirements for this setting will vary depending on the function of the platform and The Ccompany's' auditing requirements. This is the minimum setting recommended. Care must be taken when setting a larger size due to the increased risk of running out of disk space and increasing performance issues due to fragmentation etc.  NB: Maximum capacity is 4 gigabytes (GB)
Maximum security log size	81,920kb (Increase as necessary - see Control Implication)	Requirements for this setting will vary depending on the function of the platform and The Ccompany's' auditing requirements. This is the minimum setting recommended. Care must be taken when setting a larger size due to the increased risk of running out of disk space and increasing performance issues due to fragmentation etc.  NB: Maximum capacity is 4 gigabytes (GB)
Maximum system log	16,386kb	Requirements for this setting will

Control Statement	Control Procedure	Control Implication
size	(Increase as necessary - see Control Implication)	vary depending on the function of the platform and The Ccompany's' auditing requirements. This is the minimum setting recommended. Care must be taken when setting a larger size due to the increased risk of running out of disk space and increasing performance issues due to fragmentation etc.  NB: Maximum capacity is 4 gigabytes (GB)
Prevent local guest group from accessing application log	Enabled	This ensures that the guest group cannot access the application event log and should be set to ensure defence in-depth.
Prevent local guest group from accessing security log	Enabled	This ensures that the guest group cannot access the security event log and should be set to ensure defence in-depth.
Prevent local guest group from accessing system log	Enabled	This ensures that the guest group cannot access the system event log and should be set to ensure defence in-depth.
Retention method for application log	Manual (see note)	Manual retention is recommended to ensure that event logs are regularly checked. This does mean that events could be lost if the event log fills up. This setting could be altered depending on the business needs. For instance, the 'as needed' option could be used to wrap the event logs. However, as this potentially causes events to be overwritten, this may result in the loss of historical data that may be needed to conduct forensic investigations etc.
Retention method for security log	Manual (see note)	As above.
Retention method for system log	Manual (see note)	As above.

*Table 5-4: Member server event log settings*

Please note that both the Event Log setting in the Member Server and Domain Controller policies have been defined. These settings could have been just defined once in the Domain policy. This was done as these settings can be altered currently in either policy which gives greater functionality.

## System Services

Any service or application is a potential point of attack. Therefore, any unneeded services or executable files are disabled or removed to secure an environment. The following system service policy settings are recommended:

Control Statement	Control Procedure	Control Implication
Alerter	Disabled (see note)	Disabling this service can potentially break functionality in UPS alert message systems.
Application experience lookup service (AeLookupSvc)	Automatic	
Application layer gateway service (alg)	Disabled	To prevent unauthorised computers from acting as Internet Gateways. Most corporations do not use this system service – they tend to use automated software delivery apps.
Application management (appmgmt)	Disabled	
Asp .net state service (aspnet_state)	Disabled	
Automatic updates (wuauserv)	Automatic	This policy assumes that the automatic update service is required, to give the option of obtaining security patches and hot fixes from the Microsoft Windows update site. If this is incorrect and The Company's requires greater control over which critical updates are installed, then this service could be disabled.  This setting will need to be confirmed by The Company's once the relevant patch management documentation to be released by EDS has been reviewed.
Background intelligent transfer services (bits)	Manual	
Certificate services (certsvc)	Disabled	
Client service for netware (nwcworkstation)	Disabled	
Clipboard (clipsrv)	Disabled	
Cluster service (clussvc)	Disabled	
Com+ event system (comsysapp)	Manual	

Control Statement	Control Procedure	Control Implication
Com+ system application (eventsystem)	Disabled	
Computer browser (browser)	Automatic	
Cryptographic services (cryptsvc)	Automatic	If this service is stopped, key management services will stop working.
DCOM server process launcher (DcomLaunch)	Automatic	Disabling this service will stop DCOM from working.
DHCP client (dhcp)	Automatic	Disabling this service will stop servers from registering in DNS through DDNS.
DHCP server (dhcpserver)	Disabled	
Distributed file system (dfs)	Disabled	If DFS is required in the customer environment then this could set to automatic.
Distributed link tracking client (trkwks)	Disabled	
Distributed link tracking server (trksvr)	Disabled	
Distributed transaction coordinator (msdtc)	Disabled	
DNS client (dnscache)	Automatic	
DNS server (dns)	Disabled	Resolving DNS names is essential for locating DCs in AD domains.
Error reporting service (ersvc)	Disabled	Service required on DCs.
Event log (eventlog)	Automatic	When this service is disabled, users will be sent a message indicating that an error has occurred, but they will not have the option to send information to Microsoft.
Fast user switching compatibility (FastUserSwitchingCompatibility)	Manual	If the event log service is disabled it will not be possible to track events.
Fax service (fax)	Disabled	
File replication (ntfrs)	Disabled (automatic on DC)	
File server for macintosh (macfile)	Disabled	
FTP publishing service (msftpsvc)	Disabled	
Help and support (helpsvc)	Disabled	
HTTP SSL (httpfilter)	Disabled	

Control Statement	Control Procedure	Control Implication
Human interface device (hid) access (hidserv)	Disabled	
IAS jet database access (iasjet)	Disabled	
IIS admin service (iisasmin)	Disabled	
IMAPI CD - burning com service (imapiservice)	Disabled	
Indexing service (cisvc)	Disabled	
Infrared monitor (irmon)	Disabled	
Internet authentication service (ias)	Disabled	
Internet connection firewall (icf) / Internet connection sharing (ics) (sharedaccess)	Disabled	
Inter-site messaging (ismserv)	Disabled (Automatic on DC)	
IP version 6 helper service (6to4)	Disabled	
IPSec policy agent (ipsec service) (policyagent)	Automatic	
Kerberos key distribution centre (kDC)	Disabled (Automatic on DC)	
Licence logging service (licenseservice)	Disabled	
Logical disk manager (dmserver)	Manual	
Logical disk manager administrative service (dmadmin)	Manual	
Message queuing (msmq)	Disabled	
Message queuing down level clients (mqds)	Disabled	
Message queuing triggers (mqtgsvc)	Disabled	
Messenger	Disabled	
Microsoft pop3 service (pop3svc)	Disabled	
Mssql\$uddi	Disabled	
Mssqlserveradhelper	Disabled	

Control Statement	Control Procedure	Control Implication
MS software shadow copy provider (swprv)	Manual	If the customer wishes to utilise this new feature then this should be set to 'manual' at least. If the management of software-based volume shadow copies is not required, then this could be disabled.
.net framework support service (corrtsvc)	Disabled	
.net runtime optimization service (clr_optimization)	Disabled	
Netlogon	Automatic	If this service is disabled computer on the network may not authenticate users and services as ntlm authentication request would be denied.
Netmeeting remote desktop sharing (mnmsvc)	Disabled	
Network connections (netman)	Manual	
Network dde (netdde)	Disabled	
Network dde dsdm (netddedsdm)	Disabled	
Network location awareness (nla)	Manual	Disabling this service will mean dependent services will fail to start. Dependent services use the NLA service to locate networks and services.
Network provisioning service (xmlprov)	Manual	
Network news transport protocol (nntp) (nntpvc)	Disabled	
Ntlm security support provider (ntlmssp)	Automatic	The NTLM service authenticates clients that do not use Kerberos v5 authentication. If this is disabled, users cannot logon to clients using NTLM authentication protocols or access network resources.
Performance logs and alerts (sysmonlog)	Manual	
Plug and play (plugplay)	Automatic	
Portable media serial number (wmdmpmsn)	Disabled	
Print server for macintosh (macprint)	Disabled	

Control Statement	Control Procedure	Control Implication
Print spooler (spooler)	Disabled	
Protected storage (protectedstorage)	Automatic	This service protects storage of sensitive information, such as private keys. If this service is disabled then private keys will be inaccessible, certificate services will not operate, SSL and S/mime will not work, and smart card logon will fail.
QoS RSVP (RSVP)	Manual	
Remote access auto connection manager (rasauto)	Disabled	
Remote access connection manager (rasman)	Disabled	
Remote administration service (srvcscg)	Manual	This is set to manual as this service is responsible for incrementing the server boot count and raising alerts if the date and time has not been set on the server.
Remote desktop help session manager (rdsessmgr)	Disabled	
Remote installation (binlsv)	Disabled	
Remote procedure call (rpc) (rpcss)	Automatic	Disabling this service will result in operating system not loading numerous services that are dependent upon it.
Remote procedure call (rpc) locator (rpclocator)	Disabled	
Remote registry (remoteregistry)	Automatic	If this service is disabled, modifying the registry will only be allowed on the local computer. Any services that explicitly depend on this service will fail to start.
Remote server manager (appmgr)	Disabled	
Remote server monitor (appmon)	Disabled	
Remote storage notification (remote_storage_user_link)	Disabled	
Remote storage server (remote_storage_server)	Disabled	
Removable storage	Disabled	This service must be set to manual

Control Statement	Control Procedure	Control Implication
(ntmssvc)		if NTbackup is used in in the environment.
Resultant set of policy provider (rsopprov)	Disabled	
Routing and remote access (remoteaccess)	Disabled	
SAP agent (nwsapagent)	Disabled	
Secondary logon (seclogon)	Disabled	
Security accounts manager (samss)	Automatic	
Security center (wscsvc)	Automatic	
Server (lanmanserver)	Automatic	This service provides RPC support for file, print and named pipes. It therefore recommended this be set to automatic.
Shell hardware detection (shellhwdetection)	Disabled	
Simple mail transport protocol (smtp) (smtpsvc)	Disabled	
Simple tcp/ip services (simptcp)	Disabled	
Single instance storage container (groveler)	Disabled	
Smart card (scardsvr)	Disabled	
SNMP service (snmp)	Disabled	
SNMP trap service (snmptrap)	Disabled)	
Special administration console helper (sacsvr)	Disabled	
Sqlagent\$uddi	Disabled	
Sqlagent\$webdb	Disabled	
System event notification (sens)	Automatic	This service is enabled as it monitors and tracks system events, such as power events.
System restore service (srsservice)	Automatic	
Task scheduler (schedule)	Disabled	This service must be set to automatic if NTbackup (built-in backup software) is used in the environment.

Control Statement	Control Procedure	Control Implication
TCP/IP NetBIOS helper service (lmhosts)	Automatic	
TCP/IP print server (ldpsvc)	Disabled	
Telephony (tapisrv)	Disabled	
Telnet (tlntsrv)	Disabled	
Terminal services (termservice)	Automatic	As this is a powerful tool for remote administration, it is enabled. By default, Terminal Services system service is installed in Remote Admin mode.
Terminal service licensing (termservlicensing)	Disabled	
Terminal services session directory (tssdis)	Disabled	
Themes	Disabled	
Trivial FTPdaemon (tftpd)	Disabled	
Uninterruptible power supply (ups)	Disabled	
Upload manager (uploadmgr)	Disabled	
Virtual disk service (vds)	Disabled	
Volume shadow copy (vss)	Manual	
Webclient	Disabled	
Web element manager (elementmgr)	Disabled	
Windows audio (audiosrv)	Disabled	
Windows firewall / Internet connection sharing (ics) (sharedaccess)	Disabled	
Windows image acquisition (wia) (stisvc)	Disabled	
Windows installer (msiserver)	Automatic	
Windows internet name server (wins)	Disabled	
Windows management instrumentation (winmgmt)	Automatic	

Control Statement	Control Procedure	Control Implication
Windows management instrumentation driver extensions (wmi)	Manual	
Windows media services (wmserver)	Disabled	
Windows system resource manager (Windowsystemresource manager)	Disabled	
Windows time (w32time)	Automatic	Time is a key component for auditing and Kerberos v5, so this is set to automatic.
Windows user mode driver framework (UMWdf)	Automatic	
Winhttp web proxy auto-discovery service (winhttpautoproxy service)	Disabled	
Wireless configuration (wzcsvc)	Disabled	It is imperative a full security review be conducted before enabling wireless configurations due to the increased security risks.
Wmi performance adapter (wmiapsrv)	Manual	
Workstation (lanmanworkstation)	Automatic	If this service is disabled, then connections cannot be established to remote servers or files accessed through named pipes.
World wide web publishing service (w3svc)	Disabled	

*Table 5-5: Member Server services policy*

For more information concerning the above-mentioned services, please refer to appendix A.

### **System File and Registry Key Permissions**

Windows 2000 Server implemented discretionary ACLs (DACLS) for file system permissions; however, the default installation had numerous shortfalls that made the use of security templates imperative. When designing Windows 2003 Server, Microsoft took these issues onboard and now recommends that no additional System File or Registry Key Permissions are required for the base installation.

However, users with the necessary privileges are able to alter these permissions. Therefore, the DC policy resets the installation to the default permissions on application.

### **Assumptions**

The Windows 2003 server infrastructure under deployment is being developed in isolation from existing services. Therefore, the security settings defined in this policy can be defined at their most secure; as the

interoperability with legacy operating systems is not required (i.e. the functional levels for the AD and DCs are set to 'Windows Server 2003')

**Note:**

When the security standards work started interoperability with legacy environment was not required – however, the scope of GDP has changed, which means the documentation will need some alteration (in terms of the INF templates) to reflect changes for NT4 compatibility..

**Important:**

It is also assumed the installation of the Windows 2003 Server operating system will be done on a 'clean' machine and will not involve an upgrade from a legacy operating system. The clients used within this system are all Windows XP machines. Whether this assumption is correct or not, the security templates and recommended settings need to be stringently tested before being applied to a production environment.

**Registry Settings**

This section details the registry keys, which should be set to protect the server from additional local and network-based attacks.

These settings are embedded into the recommended member server security policy.

**Network Denial-of-Service Attack**

To help prevent Denial of Service (DoS) attacks networks should be kept updated with the latest security fixes and the TCP/IP protocol stack running Windows 2003 should be hardened to reduce the likelihood of an incident.

The following registry values are recommended to mitigate the risk of a network-based DoS attack:

Hive	Key	Subkey	Format	Value	Note
Hklm	\system\ccs\Services\tcpip\Parameters\	Enableicmpredirect	Dword	0	Hklm = hkey_local_machine  Ccs = currentcontrolset  This setting enforces ICMP routing by the shortest path and mitigates issues with host routes in OSPF when RRAS is configured as an ASBR (gateway to another autonomous system, i.e. not in the OSPF domain).
Hklm	\system\ccs\Services\tcpip\Parameters\Synattackprotect	Synattackprotect	Dword	1	This setting adjusts retransmission of TCP syn-ack packets in the event of a SYN DoS attack. This setting gives protection, whereas a setting of 0 does not.
Hklm	\system\ccs\Services\tcpip\Parameters\	Enabledeadgwdetect	Dword	0	This setting ensures this setting is turned off. If turned on, 1, an attacker could force internal traffic to be directed to another gateway.
Hklm	\system\ccs\	Enablepmtudiscovery	Dword	0	This setting disables this

Hive	Key	Subkey	Format	Value	Note
	Services\tcpip\ Parameters\ 				features and ensures that an MTU size of 576 bytes is used for all non-local subnet connections. This stops an attacker using a small MTU value and overworking the stack.
Hklm	\ccs\services\ Tcip\ parameters\ 	Keepalivetime	Dword	300000 (see note)	The purpose of this setting is to control how often TCP attempts to verify that an idle connection it still intact by sending a keep-alive packet. The recommended setting equates to 5 minutes and means that the inactive session will be timed out quicker. If this setting causes issues, then consider increasing to 10 minutes (600000) or even 20 minutes (1200000) on a per server basis.
Hklm	\system\ccs\ Services\tcpip\ Parameters\ 	Disableipsourcerouting	Dword	2	This protects against IP source routing spoofing. If source routing is absolutely necessary (not recommended due to security implications) then try to disable source routing with IP forwarding enabled (1). Source routing can be used to map a network and circumvent perimeter security.
Hklm	\system\ccs\ Services\tcpip\ Parameters\ 	Tcpmaxconnectresponse Retransmissions	Dword	3 (see note)	A syn attack is where an attacker or number of attackers send a continuous stream of syn packets to a server, until the server is overwhelmed by half-open connections and cannot respond to legitimate requests. This setting means half-open connections will be dropped after 21 seconds.  If the server in question is under heavy attack then this setting can be dropped to a 0 or 1. However, dropping the value this low will have an impact on legitimate connection attempts.

Hive	Key	Subkey	Format	Value	Note
Hklm	\system\ccs\Services\tcpip\Parameters\	Tcpmaxdataretransmissions	Dword	3	Used by the server to limit an syn attack by setting a retransmission timer for each outbound segment passed to IP.
Hklm	\system\ccs\Services\tcpip\Parameters\	Performrouterdiscovery	Dword	0	This disables IRDP so it cannot be used to detect gateways. The security risk is that a malicious user on the local segment could configure a device to impersonate a router. This means sensitive traffic could potentially be routed to a malicious device.
Hklm	\system\ccs\Services\tcpip\Parameters\	Tcpmaxportsexhausted	Dword	5	Used by the server to determine whether a syn attack is taking place.

Table 6-1: Registry Denial-of-Service Settings

### Perimeter Security (Against DoS)

Generally, perimeter network devices, such as routers and firewalls, give protection from an external DoS attack. If this is the case, then it is highly recommended that these devices be reviewed to provide additional protection to your network. These settings are therefore included to provide defence-in-depth and to give protection from internal hosts.

### Afd Settings

A number of Windows socket applications, such as web servers, have their connection attempts handled by the afd.sys component. The version of afd.sys released with Windows 2003 server can be configured to handle a large number of half-open connection requests, which can help to mitigate a syn attack. This is accomplished by setting up a dynamic backlog to handle these requests. The setting for the afd.sys component can be configured via four registry settings, which shown in the table below:

Hive	Key	Subkey	Format	Value	Note
Hklm	\system\ccs\Services\afd\Parameters\	Dynamicbackloggrowthdelta	Dword	10 (see note)	Hklm = hkey_local_machine  Ccs = currentcontrolset  This defines the number of extra free connections to create when additional connections are required.  This setting is a balance between providing scope to handle a syn attack but not consuming too many resources, and thus having an impact on system performance.

Hive	Key	Subkey	Format	Value	Note
Hklm	\system\ccs\Services\afd\Parameters\	Enabledynamicbacklog	Dword	1	This setting will enable dynamic backlogging. Set to 0 to disable this feature (not recommended).
Hklm	\system\ccs\Services\afd\Parameters\	Minimumdynamicbacklog	Dword	10 (see note)	This controls the number of free connections allowed on a listening endpoint. If the number of free connections drops below this value, then additional free connections are generated.  If the system is under attack or the possibility of an attack is high, this setting should be set to 20 (Microsoft recommendation). Setting this value too high will affect system performance.
Hklm	\system\ccs\Services\afd\Parameters\	Maximumdynamicbacklog	Dword	20000 (see note)	This setting depends on the memory available in the system. The value shown is the one recommended and equates to having 128Mb of RAM (5000 for each 32Mb).  If the system is under attack or if the possibility of an attack is high, this setting should be increased, but the setting is dependent on the available memory. Setting this value too high will affect system performance.

*Table 6-2: AFD settings*

### NetBIOS Name Release Security

As the NetBIOS protocol is not designed to allow authentication, it is vulnerable to spoofing techniques that could allow in a malicious user to send a namerelease request to the server, forcing it to relinquish its name. This type of attack will result in intermittent loss of services on the targeted server, such as domain logon.

This is not an issue in an environment where WINS is not present and name resolution is provided by DNS. As the use of WINS within the proposed Windows 2003 infrastructure is to be used, this registry setting is included in the table below:

Hive	Key	Subkey	Format	Value	Note
Hklm	\system\ccs\Services\netbt\Parameters	Nonamereleaseondemand	Dword	1 (see note)	Hklm = hkey_local_machine Ccs = currentcontrolset

					This determines whether the computer releases its NetBIOS name when it receives a namerelease request. It is recommended that this protection is enabled and that this setting is thoroughly tested before being made live on a production network.
--	--	--	--	--	---

Table 6-3: NetBIOS settings

### Disable Legacy Filename Support

Windows 2003 supports 8.3 (filename.ext) for backward compatibility with 16-bit applications. This means that an attacker could refer to a file by its 8.3 naming convention. For instance, thisisapasswordfile.txt would be thisis~1.txt (the ~1 refers to the first instance of this combination of 8 characters). This makes it easier for an attacker to reference filenames and run applications that have very long filenames. Disabling this will also increase directory enumeration performance on the system.

It is recommended that the following registry setting be configured to turn off 8.3 support:

Hive	Key	Subkey	Format	Value	Note
Hklm	\system\ccs\Control\FileSystem\	Ntfsdisable8dot3namecreation	Dword	1 (see note)	Hklm = hkey_local_machine  Ccs = currentcontrolset  If this setting is turned off (0) on a server where automatic 8.3 filenames are present, they will not be removed. It is recommended that this setting is thoroughly tested before being made live on a production network where 16-bit applications are in use.

Table 6-4: Legacy filename settings

### Disable Autorun

Autorun begins reading from a drive as soon as media is loaded into it. As a result, the setup file of programmes on the media and/or the sound on audio media starts immediately. To prevent a malicious programme from starting when media is loaded into a drive, add the following registry key:

Hive	Key	Subkey	Format	Value	Note
Hklm	\software\Microsoft\Windows\Currentversion\policies\explorer\	Nodrivetypeautorun	Dword	0xff	Hklm = hkey_local_machine This setting (0xff = 255 decimal) will disable autorun for all types of media, which is recommended.

Table 6-5: Autorun settings

### Screen Saver Password Protection

There is a predefined grace period from when the screen saver is launched and the screen is locked. This is to allow the user to catch the screen saver without having to re-enter the password, which is often useful on a client machine. This provides a window of opportunity (the default is 5 seconds) for a malicious user to log on to a server locally before the lock takes affect. It is therefore mandatory the registry setting detailed in the table below is implemented:

Hive	Key	Subkey	Format	Value	Note
Hklm	Software\ Microsoft\ Windowsnt\ currentversion\ winlogon\	Screensavergraceperiod	String	0	Hklm = hkey_local_machine  This setting ensures that the lock is applied immediately.

Table 6-6: Screen saver settings

### Security Log Capacity Password Message

As auditing of events, especially security related ones, is critical the following registry setting should be implemented. This will warn the administrators when the log is becoming full:

Hive	Key	Subkey	Format	Value	Note
Hklm	\system\ccs\Serv ices\ Eventlog\ Security\ 	Warninglevel	Dword	90	Hklm = hkey_local_machine  Ccs = currentcontrolset  This setting will generate a successful event entry (id 523) under the category of system in the event log when the security log is at 90% capacity. This value can be reduced if necessary (50, 60, 70 or 80 %).

Table 6-7: Security log settings

### Enable Safe DLL Search Order

If a user executes malicious code that contains modified system DLLs, this code may be able to load these DLLs onto the system and increase the range of damage it can cause. To apply a strict order in which system DLLs are searched for, apply the following registry setting:

Hive	Key	Subkey	Format	Value	Note
Hklm	\system\ccs\ 	Safedllsearchmode	Dword	1	Hklm = hkey_local_machine

	Control\ Session manager\ 			(see note)	<p>Ccs = currentcontrolset</p> <p>This setting will cause applications to search for DLLs in the system path first. For applications that require unique versions of these DLLs which are included with the application, this causes stability issues. It is therefore recommended this setting be tested before being deployed in a production environment.</p>
--	----------------------------------	--	--	---------------	--

*Table 6-8: Safe DLL search settings*

