Defense Security Service
Office of the Designated Approving Authority

Standardization of Baseline Technical Security Configurations

March 2009
Version 2.2

This page intentionally left blank.

1. Introduction....4
2. General Assumptions....4
3. System Basic....5
4. Components Overview....6
4.1 Account Policies....6
4.2 Password Policy....7
4.5 Audit Policy....21
4.6 User Rights....29
4.7 Security Options....59
5. Event Log....126
6. Restricted Groups....135
7. File System Security....138
7.1 NTFS....138
7.2 Folder Options....138
7.4 Individual File Auditing....147
8. System Services....148
8.1 Service Overview....148
8.2 Vulnerability....148
8.3 Service Settings....149
8.4 Remote Access....152
9. Registry Keys....152
10. Network Communication Ports....156
10.1 Common Ports and Services....156
10.2 Stand Alone System....157
10.3 Windows Firewall....157
10.4 Banner between network services....157
10.5 Disabling USB storage devices....157
10.6 Disabling IPv6 protocol....159
11. Conclusion....160
12. References....160

1. Introduction

The purpose of this document is to establish a baseline standard of technical security controls for information systems for the Defense Security Service's (DSS) National Industrial Security Program and its participants. The protection of classified information maintained, hosted, or processed within computer systems necessitates the need for strong technical security controls to the maximum extent possible. These Baseline Standards currently contain the specific settings for securing the Microsoft Windows operating systems. ***This document will change shortly to include other Operating Systems.*** The configuration settings are based on documentation containing a comparison of different settings recommended by **Defense Information System Agency** (DISA), **National Institute of Standards and Technology** (NIST)**, National Security Agency** (NSA), Microsoft, and **NISPOM** standards. This document will not provide the step by step recommended setting implementations, discuss some of the risks that are associated with a particular setting. A separate document will provide the step-by-step implementation for the baseline settings found in this document. In addition, an automated tool is developed that will facilitate the configurations outlined in this document.

The use of these Defense Security Service (DSS) Baseline Standards will strengthen system security controls and expedite DSS certification and accreditation reviews and on-site verifications.

2. General Assumptions

- Servers and Workstations are physically secured.
- Only system administrators are local administrators.
- Every administrator (each person) has a separate account, i.e. no shared administrator accounts.
- Installation and patching is done OFF the network, so server isn't exploited prior to patching.
- All drives are formatted NTFS.
- Email will not be read on the server by anyone.
- Remote access software will not be installed. Windows Terminal Services in application mode can be employed if remote console access is required by non-administrators.

- No account will be logged in at the console continuously. Most processes can be configured to run as a service. Processes which must be run from the console and not as a service require a locked console.

If these assumptions are not true, document the reason for the exceptions in order to facilitate Defense Security Service staff performing certification and accreditation.

3. System Basic

- Applications should not be installed on the system drive.
- User or application data should not be stored on the system drive.
- Only administrators should have access to the system drive or partitions.
- Replace Everyone ACLs with Authenticated Users, Domain Users, or a more restrictive group.
- Web browsing from a server is a security risk due to browser security issues. If browsing is required, server-based browsers should be vigilantly patched, and if possible restrictions on use should be employed.
- Any service which requires a service account which is a domain user should be documented as a known security issue. Should the server be compromised these accounts can easily be used to further compromise other domain systems. Pre-built code which will grab the password for service accounts (given a system level compromise) is easy to obtain on the internet.
- IPSec is strongly encouraged for enhanced security if all client operating systems are Windows 2000 or higher.
- Consider implementing SMB signing and secure channel encryption if all clients have an AD client.

This part of the document discusses those Group Policy settings that are applied at the Domain Level. The built-in Default Domain Controller policy includes default setting values for these policies, which are collectively referred to as Account policies.

The baseline standards and settings provide a high level of security for Windows XP Professional systems when used in conjunction with a sound and comprehensive local security policy and other relevant security controls.

4. Components Overview

This section presents an overview of the various security features offered by the Windows XP / 2003 Server operating system (OS). Many of the components have been inherited from Windows 2000, often with improvements and enhancements. Windows XP also includes several new security features.

4.1 Account Policies

There are three different types of Account policies: password policies, account lockout policies, and Kerberos authentication protocol policies. A single Microsoft Windows Server™ 2003 domain may have one of each of these policies. If these policies are set at any other level in Active Directory, only local accounts on member servers will be affected.

***Note**: For domain accounts, there can be only one Account policy per domain. The Account policy must be defined in the Default Domain Policy or in a new policy that is linked to the root of the domain and given precedence over the Default Domain Policy, which is enforced by the domain controllers that make up the domain. A domain controller always pulls the Account policy from the root of the domain, even if there is a different Account policy applied to the OU that contains the domain controller. The root of the domain is the top level container of the domain, not to be confused with the root domain in a forest; the root domain in a forest is the top level domain within that forest.*

The Account policy settings in Group Policy are all applied at the domain level. Default values are present in the built-in Default Domain Controller policy for password policies, account lockout policies, and Kerberos policies. When you configure these policies in the Active Directory® directory service, remember that Microsoft® Windows® only allows one domain Account policy—the Account policy that is applied to the root domain of the domain tree. The domain Account policy will become the default Account policy of any Windows computer that is a member of the domain.

The only exception to this rule is when another Account policy is defined for an organizational unit (OU). The Account policy settings for the OU will affect the Local Policies on any computers that are contained in the OU. For example, if an OU policy defines a maximum password age that differs from the domain-level Account policy, the OU policy will only be applied and enforced when users log on to the local computer. Only default local computer policies will apply to computers that are in a workgroup or in a domain where neither an OU Account policy nor a domain policy applies.

The settings for each of these policy types are discussed throughout this document.

4.2 Password Policy

In Windows and many other operating systems, the most common method to authenticate a user's identity is to use a secret pass phrase or password. A secure network environment requires all users to use strong passwords (ones that have at least ten characters and include a combination of letters, numbers, and symbols). These passwords help prevent the compromise of user accounts and administrative accounts by unauthorized people who use either manual methods or automated tools to guess weak passwords. Strong passwords that are changed regularly reduce the likelihood of a successful password attack. (More detailed information about strong passwords is provided in the "Passwords must meet complexity requirements" section later in this document.)

You can enforce the use of strong passwords through an appropriate password policy. Password policy settings control the complexity and lifetime of passwords. This section discusses each specific password policy account setting. You can configure the password policy settings in the following location within the Group Policy Object Editor:

Computer Configuration\Windows Settings\Security Settings\ Account Policies\Password Policy

If groups exist that require separate password policies, they should be segmented into another domain or forest based on any additional requirements.

Password Policy	Mutiuser Stand Alone (MUSA)	P2P LAN	Client/Server AD
Set the Password History Requirements ***Security Objective:*** Set limit on how often passwords may be reused. ***Vulnerability:*** Password reuse is an important concern in any organization. Many users will want to use or reuse the same password for their account over a long period of time. The longer the same password is in use for a particular account, the greater the chance that an attacker will be able to determine the password through brute-force attacks. Also, any accounts that may have been compromised will remain exploitable for as long as the password is left unchanged. If password changes are required but password reuse is not prevented, or if users can continually reuse a small number of passwords, the effectiveness of a good password policy is greatly reduced. If you specify a low number for this policy setting, users will be able to use the same small number of passwords repeatedly. If you do not also configure the **Minimum password age** setting, users will be able to repeatedly change their passwords until they can reuse their original password. ***Procedure:*** a. Double click on the **Enforce password history** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. b. Change the number in the **passwords remembered** field (maximum is 24) to reflect the number of passwords the system will remember. A recommended setting is 24 passwords remembered.	24	24	24

Password Policy	Mutiuser Stand Alone (MUSA)	P2P LAN	Client/Server AD
Set the Maximum Password Age ***Security Objective:*** Set the length of time users can keep their passwords before they have to change them. ***Vulnerability:*** Any password, even the most complex password, can be guessed (or "cracked") by an attacker with sufficient time and computer processing power. Some of the following policy settings can make it harder to crack passwords in a reasonable amount of time. The risk of a valid password being cracked can be reduced if users are frequently required to change their passwords, which can also mitigate the risk of unauthorized logon by someone who wrongfully acquired a password. You can configure the **Maximum password age** setting so that users are never required to change their passwords, but such a configuration would be a major security risk The possible values for the Maximum password age setting are: • A user-specified number of days between 0 and 999 • Not Define ***Procedure:*** a. Double click on the **Maximum password age** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. b. Change the number in the **days** field to the desired number. A recommended setting is 42 days. ***Note*:** The ST requires that the administrator be able to set a password expiration time, but does not specify an expiration period. A maximum password age must be set if a minimum password age is used.	90	90	90

Password Policy	Mutiuser Stand Alone (MUSA)	P2P LAN	Client/Server AD
Set the Minimum Password Age ***Security Objective:*** Set the length of time users must keep a password before they can change it. ***Vulnerability:*** It is ineffective to require users to change passwords regularly if they can cycle through passwords until they can reuse a favorite password. Use this policy setting with the **Enforce password history** setting to prevent the reuse of old passwords. For example, if you configure the **Enforce password history** setting to ensure that users cannot reuse any of their last 12 passwords, they could change their password 13 times in a few minutes and reuse the password they started with unless you configure the **Minimum password age** setting to a number that is greater than 0. You must configure this policy setting to a number that is greater than **0** for the **Enforce password history** setting to be effective. ***Procedure:*** a. Double click on the **Minimum password age** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. b. Change the number in the **days** field to the desired number. A recommended setting is 1 days. ***Note:*** The ST requires that the administrator be able to set a minimum password age, but does not specify the length of time users must keep a password before they can change it. A minimum password age must be set if a maximum password age is used.	1	1	1

Password Policy	Mutiuser Stand Alone (MUSA)	P2P LAN	Client/Server AD
Minimum password length ***Security Objective:*** This policy setting determines the least number of characters that may make up a password for a user account. There are many different theories about how to determine the best password length for an organization, but perhaps "pass phrase" is a better term than "password." In Microsoft Windows 2000 and later versions, pass phrases can be quite long and they can include spaces, punctuation marks, and Unicode characters. Therefore, a phrase such as "I want to drink a $5 beverage!" is a valid pass phrase. Such a phrase is considerably stronger than an 8 or 10 character string of random numbers and letters, but it is easier to remember. The possible values for the **Minimum password length** setting are: • A user-specified number between 0 and 14 • Not Defined ***Vulnerability:*** There are several types of password attacks that can be performed to obtain the password for a particular user account. These attacks include dictionary attacks (which attempt to use common words and phrases) and brute force attacks (which try every possible combination of characters). Also, attackers sometimes try to obtain the account database so they can use utilities to crack the accounts and passwords. ***Procedure:*** a. Double click on the **minimum password length** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. b. Select the **number of characters required**.	12	12	12

Password Policy	Mutiuser Stand Alone (MUSA)	P2P LAN	Client/Server AD
Set the Password Complexity Requirements ***Security Objective:*** Requires the use of a complex (strong) password. This policy will impose a requirement for a combination of alphanumeric, special, and upper and lower case characters in a password. ***Vulnerability:*** Passwords that contain only alphanumeric characters are extremely easy to crack with several publicly available utilities. To prevent passwords from being cracked, they should contain a wider range of characters. The possible values for the **Passwords must meet complexity requirements** setting are: • Enabled • Disabled • Not Defined ***Procedure:*** c. Double click on the **Passwords must meet complexity requirements** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. d. Select the **Enabled** radio button. ***Note:*** The ST does not specify password complexity requirements.	**Enabled**	**Enabled**	**Enabled**
Enable Reversible Encryption for Passwords ***Security Objective:*** The **Store password using reversible encryption for all users in the domain** setting provides support for application protocols that require knowledge of the user's password for authentication purposes. ***Vulnerability:*** This policy setting determines whether Windows Server 2003 will store passwords in a weaker format that is much more susceptible to compromise. The possible values for the **Store password using reversible encryption for all users in the domain** setting are: • Enabled • Disabled • Not Defined ***Procedure:*** Verify the default setting is "**Disabled**."	**Disabled**	**Disabled**	**Disabled**

4.3 Account Lockout Policy

More than a few unsuccessful password submissions during an attempt to log on to a computer might represent an attacker's attempts to determine an account password by trial and error. Windows Server 2003 with SP1 tracks logon attempts, and you can configure the operating system to disable the account for a preset period of time after a specified number of failed attempts. Account lockout policy settings control the threshold for this response and what action to take after the threshold is reached. You can configure the account lockout policy settings in the following location within the Group Policy Object Editor:

Computer Configuration\Windows Settings\Security Settings\ Account Policies\Account Lockout Policy

This setting will slow down a dictionary attack in which thousands of well-known passwords are tried. If the account is locked out after each invalid attempt to logon, the hacker must wait until the account is enabled again. If an account is locked out, the administrator can reset it using **Active Directory Users and Computers** for domain accounts or **Computer Management** for local accounts instead of waiting the allotted lockout duration. (NSA)

Account Lockout Policy	Multiuser Stand Alone (MUSA)	P2P LAN	Client/Server AD
Account Lockout Duration ***Security Objective:*** This policy setting determines the number of minutes that a locked-out account remains locked out before it is automatically unlocked. ***Vulnerability:*** A denial of service (DoS) condition may be created if an attacker abuses the **Account lockout threshold** and repeatedly attempts to log on with a specific account. If you configure the **Account lockout threshold** setting, the account will be locked out after the specified number of failed attempts. If you configure the **Account lockout duration** setting to **0**, then the account will remain locked out until an administrator unlocks it manually ***Procedure:*** Under Local Security Policy or Default Domain Security Policy a. Double click on the **Account** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. b. Change the number in the **Account Duration** field to set the duration of the lockout. To specify that the account will remain locked until an administrator manually unlocks it, configure the value to **0**. When the **Account lockout duration** setting is configured to a non-zero value, automated attempts to guess account passwords must wait out this interval before they resume attempts against a specific account.	15	15	15
Account lockout threshold ***Security Objective:*** This policy setting determines the number of failed logon attempts that causes a user account to become locked out. ***Vulnerability:*** Password attacks may use automated methods to try thousands or even millions of password combinations for any or all user accounts. The effectiveness of such attacks can be almost eliminated if you limit the number of failed logons that can be performed. However, it is important to note that a DoS attack could be performed on a domain that has an account lockout threshold configured. A malicious attacker could programmatically attempt a series of password attacks against all users in the organization. If the number of attempts is greater than the account lockout threshold, the attacker may be able to lock out every account. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy a. Click on the **Account Lockout** policy object. b. Double click on the **Account Lockout Threshold** Setting dialog window. c. Configure the **Account Lockout Threshold** setting to **5.**	5	5	5

Reset account lockout counter ***Security Objective:*** This policy setting determines the number of minutes that must elapse before the counter that tracks failed logon attempts and triggers account lockouts is reset to **0.** ***Vulnerability:*** Users can accidentally lock themselves out of their accounts if they mistype their password multiple times. To reduce the chance of such accidental lockouts, the **Reset account lockout counter after** setting determines the number of minutes that must elapse before the counter that tracks failed logon attempts and triggers lockouts is reset to 0.. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy a. Click on the **Account Lockout** policy object. b. Double click on the **Reset account lockout counter** Setting dialog window. c. Configure the **Reset account lockout counter** setting to **15.** ***Note:*** If an **Account lockout threshold** is defined, this reset time must be less than or equal to the **Account lockout duration** setting configuration.	15	15	15

4.4 Kerberos Policy

In Windows Server 2003 with SP1, the Kerberos authentication protocol provides the default mechanism for domain authentication services and the authorization data that is necessary for a user to access a resource and perform a task on that resource. If the lifetime of Kerberos tickets is reduced, the risk of a legitimate user's credentials being stolen and successfully used by an attacker decreases. However, authorization overhead increases.

In most environments, the Kerberos policy settings should not need to be changed. These policy settings are applied at the domain level, and the default values are configured in the Default Domain Policy GPO in a default installation of a Windows 2000 or Windows Server 2003 Active Directory domain. You can configure the Kerberos policy settings in the following location within the Group Policy Object Editor:

Computer Configuration\Windows Settings\Security Settings\ Account Policies\Kerberos Policy

Kerberos is the default authentication method used in Windows 2000 Active Directory. Since Active Directory is necessary for Kerberos authentication, the Kerberos policy only has significance for the Windows 2000 domain Group Policy Object. Therefore, for the Windows XP workstation that this document addresses, the Kerberos policies will not be defined. (NSA)

Kerberos Policy Options	Multiuser Stand Alone (MUSA)	P2P LAN	Client/Server AD
Enforce user logon restrictions ***Security Objective:*** This policy setting determines whether the Key Distribution Center (KDC) validates every request for a session ticket against the user rights policy of the user account. The possible values for the **Enforce user logon restrictions** setting are: • Enabled • Disabled • Not Defined ***Vulnerability:*** If you disable this policy setting, users could receive session tickets for services that they no longer have the right to use because the right was removed after they logged on. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy a. Double click on the **Account** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. b. Change the number in the **Kerberos Policy** field to set the field options. *c*. Select *Enforce* **user logon restrictions** to enable the option. ***Note:*** Validation of each request for a session ticket is optional, because the extra step takes time and may slow network access to services.	Not Defined	Not Defined	Disable LM NTLM v.1 or Enabled if Kerberos is used

Maximum lifetime for service ticket ***Security Objective:*** This policy setting determines the maximum amount of time (in minutes) that a granted session ticket can be used to access a particular service. The setting must be 10 minutes or greater, and less than or equal to the configuration of the **Maximum lifetime for user ticket** setting. If a client presents an expired session ticket when it requests a connection to a server, the server returns an error message and the client must request a new session ticket from the KDC. After a connection is authenticated, however, it does not matter if the session ticket remains valid. Session tickets are used only to authenticate new connections with servers. Operations are not interrupted if the session ticket that authenticated the connection expires during the connection. The possible values for the **Maximum lifetime for service ticket** setting are: • A user-defined value in minutes between 10 and 99,999. If you configure this policy setting to 0, service tickets do not expire. • Not Defined. ***Vulnerability:*** If you configure the value for the **Maximum lifetime for service ticket** setting too high, then users might be able to access network resources outside of their logon hours. Also, users whose accounts were disabled might have continued access to network services with valid service tickets that were issued before their accounts were disabled. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy a. Double click on the **Account** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. b. Change the number in the **Kerberos Policy** field to set the field options. *c.* Select Maximum lifetime for service ticket to enable the option.	Not Defined	Not Defined	Not Defined

Maximum lifetime for user ticket **Security Objective:** This policy setting determines the maximum amount of time (in hours) of a user's ticket-granting ticket (TGT). When a user's TGT expires, a new one must be requested or the existing one must be renewed. The possible values for the **Maximum lifetime for user ticket** setting are: • A user-defined value in hours between 0 and 99,999. The default value is 10 hours. • Not Defined. ***Vulnerability:*** If you configure the value for the **Maximum lifetime for user ticket** setting too high, then users might be able to access network resources outside of their logon hours. Also, users whose accounts were disabled might continue to have access to network services with valid service tickets that were issued before their accounts were disabled. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy a. Double click on the **Account** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. b. Change the number in the **Kerberos Policy** field to set the field options. *c.* Select **Maximum lifetime for user ticket** to enable the option.	Not Defined	Not Defined	10 Hours
Maximum lifetime for user ticket renew ***Security Objective:*** This policy setting determines the period of time (in days) during which a user's ticket-granting ticket (TGT) may be renewed. The possible values for the **Maximum lifetime for user ticket renewal** setting are: • A user-defined value in minutes between 0 and 99,999 • Not Defined ***Vulnerability:*** If the value for the **Maximum lifetime for user ticket renewal** setting is too high, then users may be able to renew very old user tickets. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy a. Double click on the **Account** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. b. Change the number in the **Kerberos Policy** field to set the field options. *c.* Select **Maximum lifetime for user ticket renew** to enable the option.	Not Defined	Not Defined	10080 minutes or 7days

Maximum tolerance for computer clock synchronization **Security Objective:** This policy setting determines the maximum time difference (in minutes) that the Kerberos protocol will allow between the time on the client computer's clock and the time on the Windows Server 2003–based domain controller that provides Kerberos authentication. The possible values for the **Maximum tolerance for computer clock synchronization** setting are: • A user-defined value in minutes between 1 and 99,999 • Not Defined ***Vulnerability:*** To prevent "replay attacks," the Kerberos authentication protocol uses time stamps as part of its protocol definition. For time stamps to work properly, the clocks of the client and the domain controller need to be synchronized as closely as possible. Because the clocks of two computers are often not synchronized, administrators can use this policy to establish the maximum elapsed time within which a Kerberos negotiation must complete; the elapsed time is computed from the timestamps. The value of this setting limits the maximum time difference that can be tolerated between the domain controller and the client computer. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy a. Double click on the **Account** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. b. Change the number in the **Kerberos Policy** field to set the field options. c. Configure **Maximum tolerance for computer clock synchronization** setting to 5 minutes.	Not Defined	Not Defined	5 Minutes

4.5 Audit Policy

An audit log records an entry whenever users perform certain specified actions. For example, the modification of a file or a policy can trigger an audit entry that shows the action that was performed, the associated user account, and the date and time of the action. You can audit both successful and failed attempts at actions.

The state of the operating system and applications on a computer is dynamic. For example, security levels may be temporarily changed to enable immediate resolution of an administration or network issue. However, such changes are often forgotten about and never undone. If security levels are not properly reset, a computer may no longer meet the requirements for enterprise security.

Regular security analyses enable administrators to track and determine that adequate security measures are in effect for each computer as part of an enterprise risk management program. Such analyses focus on highly specific information about all aspects of a computer that relate to security, which administrators can use to adjust the security levels. More importantly, this information can help detect any security flaws that may occur in the computer over time.

Security audits are extremely important for any enterprise network, because audit logs may provide the only indication that a security breach has occurred. If the breach is discovered some other way, proper audit settings will generate an audit log that contains important information about the breach.

Oftentimes, failure logs are much more informative than success logs because failures typically indicate errors. For example, successful logon to a computer by a user would typically be considered normal. However, if someone unsuccessfully tries to log on to a computer multiple times, it may indicate an attacker's attempt to break into the computer with someone else's account credentials. The event logs record events on the computer, and in Microsoft® Windows® operating systems, there are separate event logs for applications, security events, and system events. The Security log records audit events. The event log container of Group Policy is used to define attributes that relate to the Application, Security, and System event logs, such as maximum log size, access rights for each log, and retention settings and methods. You can configure the Audit policy settings in the following location within the Group Policy Object Editor:

Computer Configuration\Windows Settings\Security Settings
Local Policies\Audit Policy

Auditing is critical to maintaining the security of the domain. On Windows XP systems, auditing is not enabled by default. Each Windows XP system includes auditing capabilities that collect information about individual system usage. The logs collect information on applications, system, and security events. Each event that is audited in an audit policy is written to the security event log, which can be viewed with the Event Viewer. (NSA)

Audit Policy	Multiuser Stand Alone (MUSA)	P2P LAN	Client/Server AD
Audit account logon events ***Security Objective:*** This policy setting determines whether to audit each instance of user logon or logoff on a different computer than the one that records the event and validates the account. ***Vulnerability:*** This policy setting specifies whether to audit successes, audit failures, or not audit the event type at all. Success audits generate an audit entry when an account logon attempt succeeds, which is useful information for accounting purposes and for post-incident forensics so that one can determine who successfully logged into which computer. Failure audits generate an audit entry when an account logon attempt fails, which is useful for intrusion detection. However, this policy setting also creates the potential for a denial of service (DoS) attack. When the **Audit: Shut down system immediately if unable to log security audits** setting is enabled, an attacker could generate millions of logon failures, fill the Security event log, and force the computer to shut down. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **Audit** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. b. Select Local Security Setting Tab of **Audit account logon events** field to set the audit event option. ***Note:*** If you configure the **Audit account logon events** setting to **Success** on a domain controller, an entry is logged for each user who is validated against that domain controller, even though the user actually logs on to a workstation or server that is joined to the domain.	Success, Failure	Success, Failure	Success, Failure

Audit account management ***Security Objective:*** This policy setting determines whether to audit each account management event on a computer. Examples of account management events include the following: • A user account or group is created, changed, or deleted. • A user account is renamed, disabled, or enabled. • A password is set or changed. ***Vulnerability*** Success audits generate an audit entry when any account management event succeeds, and the audit setting should be enabled them on all computers in the enclave. When an organization responds to security incidents, it is critical that they be able to track who created, changed, or deleted an account. Failure audits generate an audit entry when any account management event fails. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy a. Double click on the **Audit** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. b. Select Local Security Setting Tab of **Audit account management** field to set the audit event option.	Success, Failure	Success, Failure	Success, Failure
Audit Directory Services Access ***Security Objective:*** This policy setting determines whether to audit user access of an Active Directory (AD) directory service object that has an associated system access control list (SACL). A SACL is list of users and groups for which actions on an object are to be audited on a Microsoft Windows–based network. ***Vulnerability:*** Success audits generate an audit entry when a user successfully accesses an Active Directory object that has a SACL that indicates that the user should be audited for the requested action. Failure audits generate an audit entry when a user unsuccessfully attempts to access an Active Directory object that has a SACL that requires auditing. (Both types of audit entries are created before the user is notified that the request succeeded or failed.) ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **Audit** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. b. Select Local Security Setting Tab of **Audit directory service access** field to set the audit event option. ***Note:*** You can configure a SACL on an Active Directory object through the Security tab in that object's Properties dialog box. This method is analogous to Audit object access, except that it applies only to Active Directory objects and not to file system and registry objects.	Not Defined	Not Defined	For Servers that uses AD, Failure

Audit Logon events **Security Objective:** This policy setting determines whether to audit each instance of user logon, logoff, or network connection to the computer that records the audit event. ***Vulnerability:*** Success audits generate an audit entry when a logon attempt succeeds, which is useful information for accounting purposes and for post-incident forensics so that you can determine who successfully logged on to which computer. Failure audits generate an audit entry when a logon attempt fails, which is useful for intrusion detection. However, this configuration also creates a potential DoS condition, because an attacker could generate millions of logon failures, fill the Security event log, and force the server to shut down. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **Audit** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. b. Select Local Security Setting Tab of **Audit logon events** field to set the audit event option.	Success, Failure	Success, Failure	Success, Failure

Audit Object Access **Security Objective:** This policy setting determines whether to audit the event of a user who accesses an object—for example, a file, folder, registry key, or printer—that has a SACL that specifies a requirement for auditing. ***Vulnerability*** Success audits generate an audit entry when a user successfully accesses an object that has a SACL. Failure audits generate an audit entry when a user unsuccessfully attempts to access an object that has a SACL (some failure events are to be expected during normal computer operations). For example, many applications (such as Microsoft Word) always attempt to open files with both read and write privileges. If the applications are unable to do so, they then try to open the files with read-only privileges. If you enable failure auditing and the appropriate SACL on the file, a failure event will be recorded when such an event occurs. In Microsoft Windows Server™ 2003 with Service Pack 1 (SP1), you can audit access to objects that are stored in the Internet Information server (IIS) metabase. To enable metabase object auditing, you must enable **Audit object access** on the target computer, and then set SACLs on the specific metabase objects whose access you want to audit. Configure the **Audit object access** policy setting and configure SACLs on objects, will generate a large volume of entries in the Security logs. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies c. Double click on the **Audit** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. d. Select Local Security Setting Tab of **Audit object access** field to set the audit event option. ***Note:*** You must perform a two-step process to enable the capability to audit an object, such as a file, folder, printer, or registry key, in Windows Server 2003. After you enable the audit object access policy, you must determine the objects whose access you want to monitor, and then modify their SACLs accordingly. For example, if you want to audit any attempts by users to open a particular file, you can configure a Success or Failure audit attribute directly on the file that you want to monitor for that particular event with Windows Explorer or Group Policy.	Failure	Failure	Failure

Audit Policy Change ***Security Objective:*** This policy setting determines whether to audit every incidence of a change to user rights assignment policies, Windows Firewall policies, Audit policies, or trust policies. ***Vulnerability:*** This audit information is useful for accounting purposes and can help you determine who successfully modified policies in the domain or on individual computers. Failure audits generate an audit entry when a change to user rights assignment policies, Audit policies, or trust policies fails. If you enable the **Audit policy change** setting in Windows XP with SP2 and Windows Server 2003 with SP1, logging of configuration changes for the Windows Firewall component is also enabled. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **Audit** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. b. Select Local Security Setting Tab of **Audit policy change** field to set the audit event option. ***Note:*** There exist problems with auditing successes of policy change. One such problem surfaces on the first system reboot after the "Audit: Shut down system immediately if unable to log security audits" (CrashOnAuditFail) security option is enabled. Upon reboot, the system will either blue screen or hang. Apparently, there is a problem writing a policy change event to the audit log, and thus, the system crashes. Subsequent reboots will be successful, but only an administrator can log on as designed. The administrator must then reset the **CrashOnAuditFail** registry key from 2 back to 0 or 1 in order for other users to access the system. This behavior does not exist if successful policy change audit is not enabled. (NSA)	Success, Failure	Success, Failure	Success, Failure

Audit Privilege Use ***Security Objective:*** This policy setting determines whether to audit each instance of a user who exercises a user right. ***Vulnerability:*** If you configure the **Audit privilege use** setting, you can specify whether to audit successes, audit failures, or not audit the event type at all. Success audits generate an audit entry when the exercise of a user right succeeds. Failure audits generate an audit entry when the exercise of a user right fails. If you enable this policy setting, the volume of events that is generated can be very large and the events may be difficult to sort through. You should only enable this setting if you have a plan for how you will use the information that is generated. Audit events are not generated for use of the following user rights, even if success audits or failure audits are specified for this policy setting: • Bypass traverse checking • Debug programs • Create a token object • Replace process level token • Generate security audits • Backup files and directories Restore files and directories ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies c. Double click on the **Audit** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. d. Select Local Security Setting Tab of **Audit privilege use** field to set the audit event option. ***Note:*** The Audit use of all user rights including Backup and Restore setting under Security Options will audit user rights excluded here. However, it will fill up the security event log very quickly and so is not recommended. (NSA)	Success, Failure	Success, Failure	Success, Failure

Audit Process Tracking ***Security Objective:*** This policy setting determines whether to audit detailed tracking information for events such as program activation, process exit, handle duplication, and indirect object access. ***Vulnerability:*** Success audits generate an audit entry when the process being tracked succeeds. Failure audits generate an audit entry when the process being tracked fails. If you enable **Audit process tracking** in Windows XP with SP2 and Windows Server 2003 with SP1, Windows will also log information about the operating mode and status of the Windows Firewall component. When enabled, the **Audit process tracking** setting generates a large number of events. This policy setting is typically configured to **No Auditing**. However, the information that this policy setting generates can be very beneficial during an incident response because it provides a detailed log of the processes that were started and when they were launched. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **Audit** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. b. Select Local Security Setting Tab of **Audit process tracking** field to set the audit event option. ***NOTE:*** Enabling this setting will generate many events. Use only when absolutely necessary. (NIST)	No Auditing	No Auditing	No Auditing
Audit System Events ***Security Objective:*** This policy setting determines whether to audit when a user restarts or shuts down their computer, or when an event occurs that affects either computer security or the Security log. ***Vulnerability:*** If you configure the **Audit system events** setting, you can specify whether to audit successes, audit failures, or not audit the event type at all. Success audits generate an audit entry when an event executes successfully. Failure audits generate an audit entry when an event is unsuccessful. Because few additional events are recorded if both failure and success audits are enabled for system events, and because all such events are very significant, you should configure this policy setting to **Enabled** on all computers in your organization. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **Audit** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. b. Select Local Security Setting Tab of **Audit system events** field to set the audit event option. **Note:** Tracks events that affect the entire system or the Audit log. Records events such as restart or shutdown. (NSA)	Success, Failure	Success, Failure	Success, Failure

More Information

The following links provide additional information about topics that relate to Audit policies for computers that run Windows XP with SP2 or Windows Server 2003 with SP1:

- For more Audit policy information, see the "Auditing Policy" section in the Windows Server 2003 TechCenter documentation on Microsoft TechNet at www.microsoft.com/technet/prodtechnol/windowsserver2003/library/ServerHelp/6847e72b-9c47-42ab-b3e3-691addac9f33.mspx.
- The article "HOW TO: Use Group Policy to Audit Registry Keys in Windows Server 2003" at http://support.microsoft.com/default.aspx?kbid=324739 describes how to audit access to registry keys by adding SACLs to those keys.
- The articles "Windows 2000 Security Event Descriptions (Part 1 of 2)" at http://support.microsoft.com/kb/299475/ and "Windows 2000 Security Event Descriptions (Part 2 of 2)" at http://support.microsoft.com/kb/301677/ describe the security events logged by Windows 2000 Server. They also apply to Windows Server 2003 and Windows XP.

4.6 User Rights

User rights allow users to perform tasks on a computer or a domain. User rights include *logon rights* and *privileges*. Logon rights control who is authorized to log on to a computer and how they can log on. Privileges control access to computer and domain resources, and can override permissions that have been set on specific objects. (Microsoft)

You can configure the user rights assignment settings in the following location within the Group Policy Object Editor:

Computer Configuration\Windows Settings\Security Settings\ Local Policies\User Rights Assignment

User Rights Assignments determine what actions users and groups are allowed to perform. Explicitly-granted user rights supplement implicit abilities of the user or group. Advanced user rights are assigned to Administrators or other trusted groups, who are allowed to run administrative utilities, install service packs, create printers, and install device drivers. (NSA)

User Rights Assignment	Multiuser Stand Alone	P2P LAN	Client / Server AD
Access this computer from the network ***Security Objective:*** This policy setting determines whether users can connect to the computer from the network. This capability is required by a number of network protocols, including Server Message Block (SMB)-based protocols, NetBIOS, Common Internet File System (CIFS), and Component Object Model Plus (COM+). The possible values for the **Access this computer from the network** setting are: • A user-defined list of accounts • Not Defined ***Vulnerability:*** Users who can connect from their computer to the network can access resources on target computers for which they have permission. For example, the **Access this computer from the network** user right is required for users to connect to shared printers and folders. If this user right is assigned to the **Everyone** group and some shared folders have both share and NTFS file system (NTFS) permissions configured so that the same group has read access, then anyone in the group will be able to view files in those shared folders. However, this situation is unlikely for new installations of Microsoft Windows Server™ 2003 with Service Pack 1 (SP1), because the default share and NTFS permissions in Windows Server 2003 do not include the **Everyone** group. This vulnerability may have a higher level of risk for computers that you upgrade from Windows NT® 4.0 or Windows 2000, because the default permissions for these operating systems are not as restrictive as the default permissions in Windows Server 2003. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **User Rights Assignment** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. b. Select Local Security Setting Tab of the Access **this computer from the network** Properties Sheet. Select the user group and click to add or remove users or group. Note: Networked systems may require services, thus the group Everyone may be required.	Administrators, Users	Administrators, Users	Administrators, Users

Act as part of the operating system ***Security Objective:*** This policy setting determines whether a process can assume the identity of any user and thereby gain access to the resources that the user is authorized to access. The possible values for the **Act as part of the operating system** setting are: • A user-defined list of accounts • Not Defined ***Vulnerability:*** The **Act as part of the operating system** user right is extremely powerful. Anyone with this user right can take complete control of the computer and erase evidence of their activities. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **User Rights Assignment** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. *b.* Select Local Security Setting Tab of **Act as part of the operating system** Properties Sheet. Remove Local System from the list.	None	None	None

Add workstations to domain ***Security Objective:*** This policy setting determines whether a user can add a computer to a specific domain. For it to take effect, it must be assigned so that it applies to at least one domain controller. The possible values for the **Add workstations to domain** setting are: • A user-defined list of accounts • Not Defined ***Vulnerability:*** The **Add workstations to domain** user right presents a moderate vulnerability. Users with this right could add a computer to the domain that is configured in a way that violates organizational security policies. For example, if your organization does not want its users to have administrative privileges on their computers, a user could install Windows on their computer and then add the computer to the domain. They would know the password for the local administrator account, and they could log on with that account and then add their domain account to the local **Administrators** group. **Procedure:** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **User Rights Assignment** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. b. Select Local Security Setting Tab of **Add workstations to domain** Properties Remove Authenticated Users from the list. For Domain Controller, adding systems should be performed by administrators only.	None	None	Domain Administrators Only
Adjust memory quotas for a process ***Security Objective:*** This policy setting determines whether users can adjust the maximum amount of memory that is available to a process. The possible values for the **Adjust memory quotas for a process** setting are: • A user-defined list of accounts • Not Defined ***Vulnerability:*** A user with the **Adjust memory quotas for a process** privilege can reduce the amount of memory that is available to any process, which could cause business-critical network applications to become slow or to fail. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **User Rights Assignment** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. *b.* Select Local Security Setting Tab of **Adjust memory quotas for a process** Properties. Users should not be able to perform this task	Local Service, Administrators	Network Services, Local Service, Administrators	Network Services, Local Service, Administrators

log on locally ***Security Objective:*** This policy setting determines whether a user can start an interactive session on the computer. Users who do not have this right are still able to start a remote interactive session on the computer if they have the **Allow logon through Terminal Services** right. The possible values for the **log on locally** setting are: • A user-defined list of accounts • Not Defined ***Vulnerability:*** Any account with the **Allow log on locally** user right can log on at the console of the computer. If you do not restrict this user right to legitimate users who need to be able to log on to the console of the computer, unauthorized users could download and execute malicious code to elevate their privileges. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **User Rights Assignment** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. *b.* Select Local Security Setting Tab of **Allow log on locally** Properties. Click on Add User or Groups to add user-defined list of accounts. Use Remove to remove accounts. Note: If anonymous service is required t logon, then use expressive policy to add the services or users or groups to the list.	Administrators, Authenticated Users	Administrators, Authenticated Users	Administrators, Authenticated Users
Allow log on through Terminal Services ***Security Objective:*** This policy setting determines whether users can log on to the computer through a Remote Desktop connection. The possible values for the **Allow log on through Terminal Services** setting are: • A user-defined list of accounts • Not Defined ***Vulnerability:*** Any account with the **Allow log on through Terminal Services** user right can log on to the remote console of the computer. If you do not restrict this user right to legitimate users who need to log on to the console of the computer, unauthorized users could download and execute malicious code to elevate their privileges. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **User Rights Assignment** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. *b.* Select Local Security Setting Tab of **Allow log on through Terminal Services** Properties. Remove Remote Desktop User and Administrators. Add Administrators if required.	None	None	None(Administrators if required)

Backup files and Directories ***Security Objective:*** This policy setting determines whether users can circumvent file and directory permissions to back up the computer. This user right is effective only when an application attempts access through the NTFS backup application programming interface (API) through a backup utility such as NTBACKUP.EXE. Otherwise, standard file and directory permissions apply. The possible values for the **Back up files and directories** setting are: • A user-defined list of accounts • Not Defined ***Vulnerability:*** Users who are able to back up data from a computer could take the backup media to a non-domain computer on which they have administrative privileges and restore the data. They could take ownership of the files and view any unencrypted data that is contained within the backup set. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies c. Double click on the **User Rights Assignment** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. *d.* Select Local Security Setting Tab of **Back up files and directories** Properties. Click Add or Remove to modify user-defined list of accounts. Remove Backup operator if not needed. ***Note:*** If the network makes use of the Backup Operators or similar group, also assign this right to that group. Keep in mind, however, that users who have this right have the ability to bypass ACLs. Unless **FullPrivilegeAuditing** is turned on, such access is not logged.	Administrators	Administrators	Administrators

Bypass traverse checking ***Security Objective:*** This policy setting determines whether users can pass through folders without being checked for the special access permission "Traverse Folder" when they navigate an object path in the NTFS file system or in the registry. The possible values for the **Bypass traverse checking** setting are: • A user-defined list of accounts • Not Defined ***Vulnerability:*** The default configuration for the **Bypass traverse checking** setting is to allow anyone to bypass traverse checking, and experienced Windows system administrators configure file system access control list (ACLs) accordingly. The only scenario in which the default configuration could lead to a mishap would be if the administrator who configures permissions does not understand how this policy setting works. For example, they might expect that users who are unable to access a folder will be unable to access the contents of any child folders. Such a situation is unlikely, and therefore this vulnerability presents little risk. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **User Rights Assignment** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. *b.* Select Local Security Setting Tab of **Bypass traverse checking** Properties. Click Add or Remove to modify user-defined list of accounts.	Administrators, Users	Administrators, Users	Administrators, Users

Change the system time ***Security Objective:*** This policy setting determines whether users can adjust the time on the computer's internal clock. It is not required to change the time zone or other display characteristics of the system time. The possible values for the **Change the system time** setting are: • A user-defined list of accounts • Not Defined ***Vulnerability:*** Users who can change the time on a computer could cause several problems. For example, time stamps on event log entries could be made inaccurate, time stamps on files and folders that are created or modified could be incorrect, and computers that belong to a domain may not be able to authenticate themselves or users who try to log on to the domain from them. Also, because the Kerberos authentication protocol requires that the requestor and authenticator have their clocks synchronized within an administrator-defined skew period, an attacker who changes a computer's time may cause that computer to be unable to obtain or grant Kerberos tickets. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **User Rights Assignment** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. *b.* Select Local Security Setting Tab of **Change the system time** Properties. Click Add or Remove to modify user-defined list of accounts.	Administrators	Administrators	Administrators
Create a page file ***Security Objective:*** This policy setting determines whether users can create and change the size of a page file. Specifically, it determines whether they can specify a page file size for a particular drive in the **Performance Options** box that is located on the **Advanced** tab of the **System Properties** dialog box. The possible values for the **Create a page file** setting are: • A user-defined list of accounts • Not Defined ***Vulnerability:*** 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 cause reduced computer performance. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **User Rights Assignment** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. *b.* Select Local Security Setting Tab of **Create a page file** Properties. Click Add or Remove to modify user-defined list of accounts.	Administrators	Administrators	Administrators

Create a token object ***Security Objective:*** This policy setting determines whether a process can create a token, which it can then use to gain access to any local resources when the process uses NtCreateToken() or other token-creation APIs. The possible values for the **Create a token object** setting are: • A user-defined list of accounts • Not Defined ***Vulnerability:*** The operating system examines a user's access token to determine the level of the user's privileges. Access tokens are built when users log on to the local computer or connect to a remote computer over a network. When you revoke a privilege, the change is immediately recorded, but the change is not reflected in the user's access token until the next time the user logs on or connects. 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 ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **User Rights Assignment** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. *b.* Select Local Security Setting Tab of **Create a token object** Properties. Click Add or Remove to modify user-defined list of accounts.	None	None	None
Create global objects ***Security Objective:*** This policy setting determines whether users can create global objects that are available to all sessions. Users can still create objects that are specific to their own session if they do not have this user right. The possible values for the **Create global objects** setting are: • A user-defined list of accounts • Not Defined ***Vulnerability:*** Users who can create global objects could affect processes that run under other users' sessions. This capability could lead to a variety of problems, such as application failure or data corruption. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **User Rights Assignment** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. *b.* Select Local Security Setting Tab of **Create global objects** Properties. Click Add or Remove to modify user-defined list of accounts. Select INTERACTIVE, and SERVICE account click remove. Remove Administrators if terminal services are not used.	None	None	None

Create permanent shared objects ***Security Objective:*** This policy setting determines whether users can create directory objects in the object manager. Users who have this capability can create permanent shared objects, including devices, semaphores, and mutexes. This user right is useful to kernel-mode components that extend the object namespace, and they have this user right inherently. Therefore, it is typically not necessary to specifically assign this user right to any users. The possible values for the **Create permanent shared objects** setting are: • A user-defined list of accounts • Not Defined ***Vulnerability:*** Users who have the **Create permanent shared objects** user right could create new shared objects and expose sensitive data to the network ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **User Rights Assignment** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. *b.* Select Local Security Setting Tab of **Create permanent shared objects** Properties. Click Add or Remove to modify user-defined list of accounts.	None	None	None

Debug programs ***Security Objective:*** This policy setting determines whether users can open or attach to any process, even those that they do not own. This user right provides access to sensitive and critical operating system components. The possible values for the **Debug programs** setting are: • A user-defined list of accounts • Not Defined ***Vulnerability:*** The **Debug programs** user right can be exploited to capture sensitive computer information from system memory, or to access and modify kernel or application structures. Some attack tools exploit this user right to extract hashed passwords and other private security information, or to effect rootkit code insertions. By default, the **Debug programs** user right is assigned only to administrators, which helps to mitigate the risk from this vulnerability. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **User Rights Assignment** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. *b.* Select Local Security Setting Tab of **Debug programs** Properties. Click Add or Remove to modify user-defined list of accounts. ***Note:*** Software developers working on the system may need this right to debug programs running as other users. Assign the right to developer users/groups only when necessary. Several Microsoft patches released around October 2003 required Administrators to have theDebug user right to install. This has since been changed and Administrators no longer require this right. (NSA)	None	None	None

Deny access to this computer from the network ***Security Objective:*** This policy setting determines whether users have the ability to connect to the computer from the network. The possible values for the **Deny access to this computer from the network** setting are: • A user-defined list of accounts • Not Defined. ***Vulnerability:*** Users who can log on to 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. You can explicitly deny this user right to high-risk accounts (such as the local Guest account and other accounts that have no business need to access the computer over the network) to provide an additional layer of protection. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **User Rights Assignment** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. *b.* Select Local Security Setting Tab of **Deny access to this computer from the networks** Properties. Click Add for additional accounts to deny access. ***Note:*** By default, the Guest and SUPPORT_388945a0 users are denied this right. (NSA)	Guest and other high risk accounts including SUPPORT_388945a0	Guest and other high risk accounts including SUPPORT_388945a0	Guest and other high risk accounts including SUPPORT_388945a0
Deny log on as a batch job ***Security Objective:*** This policy setting determines whether users can log on through a batch-queue facility, which is the feature in Windows Server 2003 that is used to schedule and launch jobs automatically one or more times in the future. This user right is needed for any accounts that are used to launch scheduled jobs by means of the Task Scheduler. The possible values for the **Deny log on as a batch job** setting are: • A user-defined list of accounts • Not Defined ***Vulnerability:*** Accounts that have the **Deny log on as a batch job** user right could be used to schedule jobs that could consume excessive computer resources and cause a DoS condition. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **User Rights Assignment** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. b. Select Local Security Setting Tab of **Deny log on as a batch job** Properties. Click Add for additional accounts to deny access. ***Note:*** By default, the Guest and SUPPORT_388945a0 users are denied this right. (NSA)	Guests, SUPPORT_388945a0, any service accounts	Guests, SUPPORT_388945a0, any service accounts	Guests, SUPPORT_388945a0, any service accounts

Deny log on as a service ***Security Objective:*** This policy setting determines whether users can log on as a service. The possible values for the **Deny log on as a service** setting are: • A user-defined list of accounts • Not Defined ***Vulnerability:*** Accounts that can log on as a service could be used to configure and launch new unauthorized services, such as a keylogger or other malware. The benefit of the specified countermeasure is somewhat mitigated by the fact that only users with administrative privileges can install and configure services, and an attacker who has already attained that level of access could configure the service to run with the System account. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **User Rights Assignment** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. b. Select Local Security Setting Tab of **Deny log on as a service** Properties Sheet. Click Add for additional accounts to deny access. ***Note:*** By default, the Guest and SUPPORT_388945a0 users are denied this right. (NSA)	Guests, SUPPORT_388945a0, any service accounts	Guests, SUPPORT_388945a0, any service accounts	Guests, SUPPORT_388945a0, any service accounts
Deny log on locally ***Security Objective:*** This policy setting determines whether users can log on directly at the computer's keyboard. The possible values for the **Deny log on locally** setting are: • A user-defined list of accounts • Not Defined ***Vulnerability:*** Any account with the ability to log on locally could be used to log on at the console of the computer. If this user right is not restricted to legitimate users who need to log on to the console of the computer, then unauthorized users might download and execute malicious code that elevates their privileges. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **User Rights Assignment** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. b. Select Local Security Setting Tab of **Deny log on locally** Properties. Click Add for additional accounts to deny access. ***Note:*** By default, the Guest and SUPPORT_388945a0 users are denied this right. (NSA)	Guests, SUPPORT_388945a0, any service accounts	Guests, SUPPORT_388945a0, any service accounts	Guests, SUPPORT_388945a0, any service accounts

Deny log on through Terminal Services ***Security Objective:*** This policy setting determines whether users can log on to the computer through a Remote Desktop connection. The possible values for the **Deny log on through Terminal Services** setting are: • A user-defined list of accounts • Not Defined ***Vulnerability:*** Any account with the right to log on through Terminal Services could be used to log on to the remote console of the computer. If this user right is not restricted to legitimate users who need to log on to the console of the computer, then unauthorized users might download and execute malicious code that elevates their privileges. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **User Rights Assignment** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. *b.* Select Local Security Setting Tab of **Deny log on through Terminal Services** Properties Click Add or Remove to modify user-defined list of accounts. ***Note:*** By default, the Guest and SUPPORT_388945a0 users are denied this right. (NSA)	Guests, Support_388945a0, any service accounts	Guests, Support_388945a0, any service accounts	Guests, Support_388945a0, any service accounts

Enable computer and user accounts to be trusted for delegation ***Security Objective:*** This policy setting determines whether users can change the **Trusted for Delegation** setting on a user or computer object in Active Directory. Users or computers that are assigned this user right must also have write access to the account control flags on the object. Delegation of authentication is a capability that is used by multi-tier client/server applications. It allows a front-end service to use client credentials to authenticate to a back-end service. For this configuration to be possible, both client and server must run under accounts that are trusted for delegation. The possible values for the **Enable computer and user accounts to be trusted for delegation** setting are: • A user-defined list of accounts • Not Defined ***Vulnerability:*** Misuse of the **Enable computer and user accounts to be trusted for delegation** user right could allow unauthorized users to impersonate other users on the network. An attacker could exploit this privilege to gain access to network resources and make it difficult to determine what has happened after a security incident. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **User Rights Assignment** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. *b.* Select Local Security Setting Tab of **Enable computer and user accounts to be trusted for delegation** Properties Click Add or Remove to modify user-defined list of accounts.	None	None	None

Force shutdown from a remote system ***Security Objective*:** This policy setting determines whether a user can shut down a computer from a remote location on the network. The possible values for the **Force shutdown from a remote system** setting are: • A user-defined list of accounts • Not Defined ***Vulnerability:*** Any user who can shut down a computer could cause a DoS condition to occur. Therefore, this user right should be tightly restricted. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **User Rights Assignment** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. *b.* Select Local Security Setting tab of **Force shutdown from a remote system** Properties. Click Add or Remove to modify user-defined list of accounts.	None	None, Administrators	None, Administrators
Generate security audits ***Security Objective:*** This policy setting determines whether a process can generate audit records in the Security log. You can use the information in the Security log to trace unauthorized computer access. The possible values for the **Generate security audits** setting are: • A user-defined list of accounts • Not Defined ***Vulnerability:*** Accounts that can 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 unauthorized activities. If the computer is configured to shut down when it is unable to write to the Security log and it is not configured to automatically back up the log files, this method could be used to create a denial of service. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **User Rights Assignment** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. *b*. Select Local Security Setting tab of **Generate security audits** Properties. Click Add or Remove to modify user-defined list of accounts.	Network Service, Local Service	Network Service, Local Service	Network Service, Local Service

Enable computer and user accounts to be trusted for delegation ***Security Objective:*** This policy setting determines whether a process can generate audit records in the Security log. You can use the information in the Security log to trace unauthorized computer access. The possible values for the **Generate security audits** setting are: • A user-defined list of accounts • Not Defined ***Vulnerability*** Accounts that can 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 unauthorized activities. If the computer is configured to shut down when it is unable to write to the Security log and it is not configured to automatically back up the log files, this method could be used to create a denial of service. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **User Rights Assignment** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. b. Select Local Security Setting tab of **Generate security audits** Properties. Click Add or Remove to modify user-defined list of accounts.	None	None	None

Impersonate a client after authentication ***Security Objective:*** The **Impersonate a client after authentication** user right allows programs that run on behalf of a user to impersonate that user (or another specified account) so that they can act on behalf of the user. If this user right is required for this kind of impersonation, an unauthorized user will not be able to convince a client to connect—for example, by remote procedure call (RPC) or named pipes—to a service that they have created to impersonate that client, which could elevate the unauthorized user's permissions to administrative or system levels. Services that are started by the Service Control Manager have the built-in **Service** group added by default to their access tokens. COM servers that are started by the COM infrastructure and configured to run under a specific account also have the **Service** group added to their access tokens. As a result, these processes are assigned this user right when they are started. Also, a user can impersonate an access token if any of the following conditions exist: • The access token that is being impersonated is for this user. • The user, in this logon session, logged on to the network with explicit credentials to create the access token. • The requested level is less than Impersonate, such as Anonymous or Identify. Because of these factors, users do not usually need to have this user right assigned. The possible values for the **Impersonate a client after authentication** setting are: • A user-defined list of accounts • Not Defined ***Vulnerability:*** An attacker with the **Impersonate a client after authentication** user right could create a service, trick a client to make them connect to the service, and then impersonate that client to elevate the attacker's level of access to that of the client. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **User Rights Assignment** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. b. Select Local Security Setting tab of **Impersonate a client after authentication** Properties. Click Add or Remove to modify user-defined list of accounts.	Administrators	Administrators	Administrators

Increase scheduling priority ***Security Objective:*** This policy setting determines whether users can increase the base priority class of a process. (It is not a privileged operation to increase relative priority within a priority class.) This user right is not required by administrative tools that are supplied with the operating system but might be required by software development tools. The possible values for the **Increase scheduling priority** setting are: • A user-defined list of accounts • Not Defined ***Vulnerability:*** A user who is assigned this user right could increase the scheduling priority of a process to Real-Time, which would leave little processing time for all other processes and could lead to a DoS condition. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **User Rights Assignment** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. *b.* Select Local Security Setting Tab of **Increase scheduling priority** Properties. Click Add or Remove to modify user-defined list of accounts..	None	None	Administrators, Services

Load and unload device drivers ***Security Objective:*** This policy setting determines whether users can dynamically load and unload device drivers. This user right is not required if a signed driver for the new hardware already exists in the Driver.cab file on the computer. The possible values for the **Load and unload device drivers** setting are: • A user-defined list of accounts • Not Defined ***Vulnerability:*** Device drivers run as highly privileged code. A user who has the **Load and unload device drivers** user right could unintentionally install malicious code that masquerades as a device driver. Administrators should exercise greater care and install only drivers with verified digital signatures. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **User Rights Assignment** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. *b.* Select Local Security Setting Tab of **Load and unload device drivers** Properties. Click Add or Remove to modify user-defined list of accounts. ***Note:*** You must have this user right, and also be a member of either **Administrators** or **Power Users**, to install a new driver for a local printer or to manage a local printer and configure defaults for options such as duplex printing. The requirement to have both the user right and membership in **Administrators** or **Power Users** is new to Windows XP and Windows Server 2003.	Administrators	Administrators	Administrators

Lock pages in memory ***Security Objective:*** This policy setting determines whether a process can keep data in physical memory, which prevents the computer from paging the data to virtual memory on disk. If you assign this user right, significant degradation of computer performance can occur. The possible values for the **Lock pages in memory** setting are: • A user-defined list of accounts • Not Defined ***Vulnerability:*** Users with the **Lock pages in memory** user right could assign physical memory to several processes, which could leave little or no RAM for other processes and result in a DoS condition. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **User Rights Assignment** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. b. Select Local Security Setting Tab of **Lock pages in memory** Properties. Click Add or Remove to modify user-defined list of accounts.	None	None	None
Log on as a batch job ***Security Objective:*** This policy setting determines whether users can log on through a batch-queue facility such as the Task Scheduler service. When an administrator uses the Add Scheduled Task wizard to schedule a task to run under a particular user name and password, that user is automatically assigned the **Log on as a batch job** user right. When the scheduled time arrives, the Task Scheduler service logs the user on as a batch job instead of as an interactive user, and the task runs in the user's security context. The possible values for the **Log on as a batch job** setting are: • A user-defined list of accounts • Not Defined ***Vulnerability*** The **Log on as a batch job** user right presents a low-risk vulnerability. For most organizations, the default settings are sufficient. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **User Rights Assignment** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. *b.* Select Local Security Setting Tab of the **Log on as a batch job** Properties. Click Add or Remove to modify user-defined list of accounts.	None	None	None

Log on as a service ***Security Objective:*** This policy setting determines whether a security principal can log on as a service. Services can be configured to run under the Local System, Local Service, or Network Service accounts, which have a built-in right to log on as a service. Any service that runs under a separate user account must be assigned this user right. The possible values for the **Log on as a service** setting are: • A user-defined list of accounts • Not Defined ***Vulnerability:*** **Log on as a service** is a powerful user right because it allows accounts to launch network services or services that run continuously on a computer, even when no one is logged on to the console. The risk is reduced 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. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **User Rights Assignment** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. *b.* Select Local Security Setting Tab of **Log on as a service** Properties Click to Add or Remove to modify user defined list accounts	Local Service, Network Service	Local Service, Network Service	Local Service, Network Service
Log on locally ***Security Objective:*** Allows a user to log on at a system's console. The possible values for the **Log on locally** setting are: • A user-defined list of accounts • Not Defined ***Vulnerability:*** Any account with the ability to log on locally could be used to log on at the console of the computer. If this user right is not restricted to legitimate users who need to log on to the console of the computer, then unauthorized users might download and execute malicious code that elevates their privileges. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **User Rights Assignment** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. *b.* Select Local Security Setting Tab of **Log on locally** Properties Click to Add or Remove to modify user defined list accounts	Users, Administrators	Users, Administrators	Users, Administrators

Manage auditing and security log ***Security Objective:*** This policy setting determines whether users can specify object access audit options for individual resources such as files, Active Directory objects, and registry keys. Object access audits are not performed unless you enable them through **Audit Policy**, which is located under **Security Settings**, **Local Policies**. A user who is assigned this user right can also view and clear the Security event log from Event Viewer. The possible values for the **Manage auditing and security log** setting are: • A user-defined list of accounts • Not Defined ***Vulnerability:*** The ability to manage the Security event log is a powerful user right and it should be closely guarded. Anyone with this user right can clear the Security log to erase important evidence of unauthorized activity. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **User Rights Assignment** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. *b.* Select Local Security Setting Tab of **Manage auditing and security log** Properties Click to Add or Remove to modify user defined list accounts ***Note:*** This right does not allow a user to enable file and object access auditing in general. Object auditing is enabled by setting the "Audit object access" items under Audit Policies. **Administrators** Modify firmware environment variables.	Administrators,	Administrators,	Administrators

Modify firmware environment values ***Security Objective:*** This policy setting determines whether users can modify system environment variables by either a process through an API or by a user through System Properties. The possible values for the **Modify firmware environment values** setting are: • A user-defined list of accounts • Not Defined ***Vulnerability*** Anyone who is assigned the **Modify firmware environment values** user right could configure the settings of a hardware component to cause it to fail, which could lead to data corruption or a DoS condition. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **User Rights Assignment** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. *b.* Select Local Security Tab of **Modify firmware environment values** Properties Click to Add or Remove to modify user defined list accounts	Administrators	Administrators	Administrators
Perform volume maintenance tasks ***Security Objective:*** This policy setting determines whether non-administrative or remote users can perform volume or disk management tasks, such as defragment an existing volume, create or remove volumes, and run the Disk Cleanup tool. Windows Server 2003 checks for this user right in a user's access token when a process that runs in the user's security context calls SetFileValidData(). The possible values for the **Perform volume maintenance tasks** setting are: • A user-defined list of accounts • Not Defined ***Vulnerability:*** A user who is assigned the **Perform volume maintenance tasks** user right could delete a volume, which could result in the loss of data or a DoS condition. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **User Rights Assignment** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. *b.* Select Local Security Tab of the **Perform volume maintenance tasks** Properties Click to Add or Remove to modify user defined list accounts	Administrators	Administrators	Administrators

Profile single process ***Security Objective:*** This policy setting determines whether users can sample the performance of an application process. Typically, you do not need this user right to use the Microsoft Management Console (MMC) Performance snap-in. However, you do need this user right if System Monitor is configured to collect data through Windows Management Instrumentation (WMI). The possible values for the **Profile single process** setting are: • A user-defined list of accounts • Not Defined ***Vulnerability:*** The **Profile single process** user right presents a moderate vulnerability. An attacker with this user right 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 run on the computer so that they could identify countermeasures that they may need to avoid, such as antivirus software, an intrusion-detection system, or which other users are logged on to a computer. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **User Rights Assignment** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. *b.* Select Local Security Setting Tab of **Profile single process** Properties Click to Add or Remove to modify user defined list accounts ***Note:*** Software developers working on the system may need this right. Assign the right to developer users/groups only when necessary. (NSA)	Administrators	Administrators	Administrators

Profile system performance ***Security Objective:*** This policy setting determines whether a user can sample the performance of computer system processes. This privilege is required by the MMC Performance snap-in only if it is configured to collect data through WMI. Typically, you do not need this user right to use the Performance snap-in. However, you do need this user right if System Monitor is configured to collect data through WMI. The possible values for the **Profile system performance** setting are: • A user-defined list of accounts • Not Defined ***Vulnerability:*** The **Profile system performance** user right presents a moderate vulnerability. An attacker with this user right 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 active on the computer so that they could identify countermeasures that they may need to avoid, such as antivirus software or an intrusion detection system. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **User Rights Assignment** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. *b.* Select Local Security Setting **Profile system performance** Properties Click to Add or Remove to modify user defined list accounts	Administrators	Administrators	Administrators

Remove computer from docking station ***Security Objective:*** This policy setting determines whether the user of a portable computer can click **Eject PC** on the **Start** menu to undock the computer. The possible values for the **Remove computer from docking station** setting are: • A user-defined list of accounts • Not Defined ***Vulnerability:*** Anyone who has the **Remove computer from docking station** user right can remove a portable computer from its docking station. The value of this countermeasure is reduced by the following factors: • If an attacker can restart the computer, they could remove it from the docking station after the BIOS starts but before the operating system launches. • This setting does not affect servers, because they typically are not installed in docking stations. • An attacker could steal the computer and the docking station together. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **User Rights Assignment** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. *b.* Select Local Security Setting Tab of **Remove computer from docking station** Properties Click to Add or Remove to modify user defined list accounts	Administrators, Users	Administrators, Users	Administrators, Users
Replace a process level token ***Security Objective:*** This policy setting determines whether a parent process can replace the access token that is associated with a child process. The possible values for the **Replace a process level token** setting are: • A user-defined list of accounts • Not Defined ***Vulnerability:*** A user with the **Replace a process level token** privilege is able to launch processes as other users. They could use this method to hide their unauthorized actions on the computer. (On Windows 2000 computers, use of the **Replace a process level token** user right also requires the user to have the **Adjust memory quotas for a process** user right that is discussed earlier.) ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **User Rights Assignment** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. *b.* Select Local Security Setting Tab of **Replace a process level token** Properties Click to Add or Remove to modify user defined list accounts .	Local Service, Network Service	Local Service, Network Service	Local Service, Network Service

Restore files and directories ***Security Objective:*** This policy setting determines whether a user can circumvent file and directory permissions when they restore backed up files and directories and whether they can set any valid security principal as the owner of an object. The possible values for the **Restore files and directories** setting are: • A user-defined list of accounts • Not Defined ***Vulnerability:*** An attacker with the **Restore files and directories** user right could restore sensitive data to a computer and overwrite data that is more recent, which could lead to loss of important data, data corruption, or a denial of service. An attacker could overwrite executable files that are used by legitimate administrators or system services with versions that include malicious code to grant themselves elevated privileges, compromise data, or install backdoors for continued access to the computer. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **User Rights Assignment** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. *b.* Select Local Security Setting **Restore files and directories** Properties Click to Add or Remove to modify user defined list accounts ***Note:*** Even if this countermeasure is configured, an attacker could still restore data to a computer in a domain that is controlled by the attacker. Therefore, it is critical that organizations carefully protect the media that are used to back up data.	Administrators	Administrators	Administrators

Shut down the system ***Security Objective:*** This policy setting determines whether a user can shut down the local computer. The possible values for the **Shut down the system** setting are: • A user-defined list of accounts • Not Defined ***Vulnerability:*** The ability to shut down domain controllers should be limited to a very small number of trusted administrators. Although the **Shut down the system** user right requires the ability to log on to the server, you should be very careful about the accounts and groups that you allow to shut down a domain controller. When a domain controller is shut down it is no longer available to process logons, serve Group Policy, and answer Lightweight Directory Access Protocol (LDAP) queries. If you shut down domain controllers that possess Flexible Single–Master Operations (FSMO) roles you can disable key domain functionality, such as processing logons for new passwords—the Primary Domain Controller (PDC) Emulator role. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **User Rights Assignment** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. *b.* Select Local Security Setting Tab of **Shut down the system** Properties Click to Add or Remove to modify user defined list accounts	Administrators, Users	Administrators, Users	Administrators, Users

Synchronize directory service data ***Security Objective:*** This policy setting determines whether a process can read all objects and properties in the directory, regardless of the protection on the objects and properties. This privilege is required to use LDAP directory synchronization (dirsync) services. The possible values for the **Synchronize directory service data** setting are: • A user-defined list of accounts • Not Defined ***Vulnerability:*** The Synchronize directory service data user right affects domain controllers; only domain controllers should be able to synchronize directory service data. Domain controllers have this user right inherently, because the synchronization process runs in the context of the System account on domain controllers. An attacker who has this user right can view all information stored within the directory. They could then use some of that information to facilitate additional attacks or expose sensitive data, such as direct telephone numbers or physical addresses. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **User Rights Assignment** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. *b.* Select Local Security Setting Tab of **Synchronize directory service data** Properties Click to Add or Remove to modify user defined list accounts.	None	None	Domain Administrators
Take ownership of files or other objects ***Security Objective:*** This policy setting determines whether a user can take ownership of any securable object in the computer, including Active Directory objects, NTFS files and folders, printers, registry keys, services, processes, and threads. The possible values for the **Take ownership of files or other objects** setting are: • A user-defined list of accounts • Not Defined ***Vulnerability:*** Any user with the Take ownership of files or other objects user right can take control of any object, regardless of the permissions on that object, and then make any changes they wish to that object. Such changes could result in exposure of data, corruption of data, or a DoS condition. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **User Rights Assignment** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. *b.* Select Local Security Setting Tab of **Take ownership of files or other objects** Properties Click to Add or Remove to modify user defined list accounts .	Administrators	Administrators	Administrators

More Information

The following links provide additional information about user rights assignment in Windows Server 2003 and Windows XP.

- Extensive information about assigning user rights with the SCE is available in the "User Rights Assignment" section of the Security Configuration Editor online help for Windows Server 2003 at www.microsoft.com/technet/prodtechnol/windowsserver2003/library/serverhelp/71b2772f-e3c0-4134-b7f0-54c244ee9aef.mspx.
- Detailed information about local user rights assignments on Windows XP computers is available in the help topic "To assign user rights for your local computer" at www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/lpe_assign_user_right.mspx.
- For more information about user rights assignments in Windows XP, see the "User Rights Assignment" section of the online Windows XP Professional documentation at www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/uratopnode.mspx.
- For more information about how to customize the Security Configuration Editor user interface, see the Microsoft Knowledge Base article "How to Add Custom Registry Settings to Security Configuration Editor" at http://support.microsoft.com/?scid=214752.
- For more information about how to create custom administrative template files in Windows, see the Microsoft Knowledge Base article "How to: Create Custom Administrative Templates in Windows 2000" at http://support.microsoft.com/?scid=323639.

4.7 Security Options

The Security Options section of Group Policy enables or disables computer security settings for digital data signatures, Administrator and Guest account names, access to floppy disk and CD-ROM drives, driver installation behavior, and logon prompts.

You can configure the security options settings in the following location within the Group Policy Object Editor:

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options

Security Options	Multiuser Stand Alone (MUSA)	P2P LAN	client/Server AD
Accounts: Administrator account status ***Security Objective:*** This policy setting enables or disables the Administrator account for normal operational conditions. If you start a computer in safe mode, the Administrator account is always enabled, regardless of how you configure this policy setting. The possible values for the **Accounts: Administrator account status** setting are: • Enabled • Disabled • Not Defined ***Vulnerability:*** In some organizations, it can be a daunting management challenge to maintain a regular schedule for periodic password changes for local accounts. Therefore, you may want to disable the built-in Administrator account instead of relying on regular password changes to protect it from attack. Another reason to disable this built-in account is that it cannot be locked out no matter how many failed logons it accrues, which makes it a prime target for brute force attacks that attempt to guess passwords. Also, this account has a well-known security identifier (SID) and there are third-party tools that allow authentication by using the SID rather than the account name. This capability means that even if you rename the Administrator account, an attacker could launch a brute force attack by using the SID to log on. **Procedure:** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **Security Options** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. *b.* Select Local Security Setting Tab of **Accounts: Administrator account status** policy to set the radio options to Enable. ***NOTE:*** Most security options are set via a registry key. The associated registry keys are listed for each item. Those options not containing a registry key are instead secured at the API level.	Enabled	Enabled	Enabled

Security Options	Multiuser Stand Alone (MUSA)	P2P LAN	client/Server AD
Accounts: Guest account status ***Security Objective:*** This policy setting determines whether the Guest account is enabled or disabled. The possible values for the **Accounts: Guest account status** setting are: • Enabled • Disabled • Not Defined ***Vulnerability:*** The default Guest account allows unauthenticated network users to log on as Guest with no password. These unauthorized users could access any resources that are accessible to the Guest account over the network. This capability means that any network shares with permissions that allow access to the Guest account, the **Guests** group, or the **Everyone** group will be accessible over the network, which could lead to the exposure or corruption of data. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **Security Options policy** object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. *b.* Select Local Security Setting Tab of **Accounts: Guest account status** policy to set the radio options to Disable. ***NOTE:*** If the Guest account is disabled and the security option, "Network access: Sharing and security model for local accounts" is set to "Guest Only," network logons, such as those performed by the SMB Service, will fail.(NSA)	Disabled	Disabled	Disabled

Security Options	Multiuser Stand Alone (MUSA)	P2P LAN	client/Server AD
Accounts: Limit local account use of blank passwords to console logon only ***Security Objective:*** This policy setting determines whether remote interactive logons by network services such as Terminal Services, Telnet, and File Transfer Protocol (FTP) are allowed for local accounts that have blank passwords. If you enable this policy setting, a local account must have a non-blank password to perform an interactive or network logon from a remote client. The possible values for the **Accounts: Limit local account use of blank passwords to console logon only** setting are: • Enabled • Disabled • Not Defined *Note:* This policy setting does not affect interactive logons that are performed physically at the console or logons that use domain accounts. **Caution**: It is possible for third-party applications that use remote interactive logons to bypass this policy setting. ***Vulnerability:*** Blank passwords are a serious threat to computer security and should be forbidden through both organizational policy and suitable technical measures. In fact, the default settings for Windows Server 2003 Active Directory® directory service domains require complex passwords of at least seven characters. However, if a user with the ability to create new accounts bypasses your domain-based password policies, they could create accounts with blank passwords. For example, a user could build a stand-alone computer, create one or more accounts with blank passwords, and then join the computer to the domain. The local accounts with blank passwords would still function. Anyone who knows the name of one of these unprotected accounts could then use it to log on. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **Security Options policy** object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. *b.* Select Local Security Setting Tab of **blank passwords to console logon only** field to set the radio options to Enable. **Note:** This setting only affects local accounts. It does not affect domain accounts. HKLM\System\CurrentControlSet\Control\Lsa\LimitBlankPasswordUse = 1(NSA)	Enabled	Enabled	Enabled

Security Options	Multiuser Stand Alone (MUSA)	P2P LAN	client/Server AD
Accounts: Rename administrator account ***Security Objective:*** This policy setting determines whether a different account name is associated with the SID for the Administrator account. The possible values for the **Accounts: Rename administrator account** setting are: • User-defined text • Not Defined ***Vulnerability:*** The Administrator account exists on all computers that run the Windows 2000, Windows Server 2003, or Windows XP Professional operating systems. If you rename this account, it is slightly more difficult for unauthorized persons to guess this privileged user name and password combination. The built-in Administrator account cannot be locked out, regardless of how many times an attacker might use a bad password. This capability makes the Administrator account a popular target for brute force attacks that attempt to guess passwords. The value of this countermeasure is lessened because this account has a well-known SID, and there are third-party tools that allow authentication by using the SID rather than the account name. Therefore, even if you rename the Administrator account, an attacker could launch a brute force attack by using the SID to log on. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **Security Options policy** object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. *b.* Select Local Security Setting Tab of **Accounts: Rename administrator account** policy to set the options by entering the new account name in the text field. ***Note:*** If anonymous accounts are not restricted from enumerating users on the system, renaming the administrator account will have limited benefit. However, if the anonymous user is prohibited from gathering account information, renaming the administrator account is provides much more benefit. See security options affecting anonymous privileges in the Network Access section of this table. (NSA)	Rename to contractor's standard	Rename to contractor's standard	Rename to contractor's standard

Security Options	Multiuser Stand Alone (MUSA)	P2P LAN	client/Server AD
Accounts: Rename Guest account ***Security Objective:*** The **Accounts: Rename guest account** setting determines whether a different account name is associated with the SID for the Guest account. The possible values for this Group Policy setting are: • User-defined text • Not Defined ***Vulnerability:*** The Guest account exists on all computers that run the Windows 2000, Windows Server 2003, or Windows XP Professional operating systems. If you rename this account. It is slightly more difficult for unauthorized persons to guess this privileged user name and password combination. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **Security Options policy** object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. *b.* Select Local Security Setting Tab of **Accounts: Rename Guest account** policy to set the options by entering the new account name in the text field.	Rename to contractor's standard	Rename to contractor's standard	Rename to contractor's standard

Security Options	Multiuser Stand Alone (MUSA)	P2P LAN	client/Server AD
Audit: Audit the access of global system objects ***Security Objective:*** If you enable this policy setting, a default system access control list (SACL) will be applied when the computer creates system objects such as mutexes, events, semaphores, and MS-DOS® devices. If you also enable the **Audit object access** audit setting as described in this document, access to these system objects is audited. Global system objects, also known as "base system objects" or "base named objects," are ephemeral kernel objects that have had names assigned to them by the application or system component that created them. These objects are most commonly used to synchronize multiple applications or multiple parts of a complex application. Because they have names, these objects are global in scope, and therefore visible to all processes on the computer. These objects all have a security descriptor but typically have a NULL SACL. If you enable this policy setting at startup time, the kernel will assign a SACL to these objects when they are created. The possible values for the **Audit: Audit the access of global system objects** setting are: • Enabled • Disabled • Not Defined ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **Security Options policy** object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. *b.* Select Local Security Setting Tab of **system objects field** policy to set the radio options of Disable. ***Note:*** Enabling this option will result in large numbers of events being written to the security logs. Coupled with the fact that global system audit events are difficult to decipher, it is recommended that this option be enabled only when deemed absolutely necessary. To audit access to system objects, the "Audit object access" audit policy must be enabled.	Disabled	Disabled	Disabled

Security Options	Multiuser Stand Alone (MUSA)	P2P LAN	client/Server AD
Audit: Audit the use of Backup and Restore privilege ***Security Objective:*** This policy setting determines whether to audit the use of all user privileges, including Backup and Restore, when the **Audit privilege use** setting is in effect. If you enable both policy settings, an audit event is generated for every file that is backed up or restored. If you enable this policy setting in conjunction with the **Audit privilege use** setting, any exercise of user rights in the Security log is recorded. If you disable this policy setting, actions by users of Backup or Restore privileges are not audited, even if **Audit privilege use** is enabled. The possible values for the **Audit: Audit the use of Backup and Restore privilege** setting are: • Enabled • Disabled • Not Defined ***Vulnerability:*** If you enable this option when the **Audit privilege use** setting is also enabled, an audit event is generated for every file that is backed up or restored. This information could help you to identify an account that was used to accidentally or maliciously restore data in an unauthorized manner. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **Security Options policy** object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. *b.* Select Local Security Setting Tab of **Audit: Audit the use of Backup and Restore privilege** policy to set to Disabled. ***Note:*** To audit user rights, the "Audit privilege use" audit policy must be enabled. HKLM\System\CurrentControlSet\Control\Lsa\FullPrivilegeAuditing	Disabled	Disabled	Disabled

Security Options	Multiuser Stand Alone (MUSA)	P2P LAN	client/Server AD
Audit: Shut down system immediately if unable to log security audits ***Security Objective:*** This policy setting determines whether the computer shuts down if it is unable to log security events. The Trusted Computer System Evaluation Criteria (TCSEC)-C2 and Common Criteria certifications require that the computer be able to prevent the occurrence of auditable events if the audit system is unable to log them. The way that Microsoft chose to meet this requirement is to halt the computer and display a stop message in the case of a failure of the audit system. If you enable this policy setting, the computer stops if a security audit cannot be logged for any reason. Typically, an event fails to be logged when the Security event log is full and its specified retention method is either **Do Not Overwrite Events** or **Overwrite Events by Days**. When this policy setting is enabled, the following **Stop** message displays if the security log is full and an existing entry cannot be overwritten: STOP: C0000244 {Audit Failed} An attempt to generate a security audit failed. To recover, an administrator must log on, archive the log (optional), clear the log, and disable this option to allow the computer to be restarted. At that point, it may be necessary to manually clear the Security event log before you can configure this policy setting to **Enabled**. The possible values for the **Audit: Shut down system immediately if unable to log security audits** setting are: • Enabled • Disabled • Not Defined ***Vulnerability:*** 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. Also, an attacker could potentially generate a large volume of Security event log messages to purposely force a computer shutdown. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **Security Options policy** object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. *b.* Select Local Security Setting tab of **Audit: Shut down system immediately if unable to log security audits** policy to set the radio option to Enable. ***Note:*** It is generally recommended that this setting be enabled; however due to a problem that exists with auditing successful policy changes we are recommending that this setting be disabled until the issue is resolved. The problem surfaces on the first system reboot after the "Audit: Shut down system immediately if unable to log security audits" security option is enabled. Upon reboot, the system will either blue screen or hang. Apparently, there is a problem writing a policy change event to the audit log, and thus, the system crashes. Subsequent reboots will be successful. When the machine reboots, only an administrator can log on. The administrator must then reset the CrashOnAuditFail registry key from 2 back to 0 or 1 in order for other users to access the system. This behavior does not exist if successful policy change audit is not enabled. (NSA) HKLM\System\CurrentControlSet\Control\Lsa\CrashOnAuditFail =0	Enabled	Enabled	Enabled

Security Options	Multiuser Stand Alone (MUSA)	P2P LAN	client/Server AD
DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL)	Not Defined	Not Defined	Not Defined
Security Objective: This policy setting allows administrators to define additional computer-wide access controls that govern access to all Distributed Component Object Model (DCOM)–based applications on a computer. These controls restrict call, activation, or launch requests on the computer. The simplest way to think about these access controls is as an additional access check call that is done against a computer-wide access control list (ACL) on each call, activation, or launch of any COM server on the computer. If the access check fails, the call, activation, or launch request will be denied. (This check is in addition to any access check that is run against the server-specific ACLs.) In effect, it provides a minimum authorization standard that must be passed to access any COM server on the computer. The **DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL)** setting controls access permissions to cover call rights. These computer-wide ACLs provide a way to override weak security settings that are specified by a specific application through CoInitializeSecurity or application-specific security settings. They provide a minimum security standard that must be passed, regardless of the settings of the specific server. These ACLs provide a centralized location for an administrator to set general authorization policy that applies to all COM servers on the computer. The **DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL)** setting allows you to specify an ACL in two different ways. You can type in the security descriptor in SDDL, or you can choose users and groups and grant or deny them Local Access and Remote Access permissions. Microsoft recommends that you use the built-in user interface to specify the ACL contents that you want to apply with this setting. ***Vulnerability:*** Many COM applications include some security-specific code (for example, to call CoInitializeSecurity) but use weak settings that often allow unauthenticated access to the process. Administrators cannot override these settings to force stronger security in earlier versions of Windows without modification of the application. An attacker could attempt to exploit weak security in an individual application by attacking it through COM calls. Also, COM infrastructure includes the RPCSS, a system service that runs during computer startup and always runs after that. This service manages activation of COM objects and the running object table, and provides helper services to DCOM remote. It exposes RPC interfaces that can be called remotely. Because some COM servers allow unauthenticated remote access (as explained in the previous section), these interfaces can be called by anyone, including unauthenticated users. As a result, RPCSS can be attacked by malicious users who use remote, unauthenticated computers. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **Security Options policy** object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. *b.* Select Local Security Setting Tab **DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL)** Press Edit Security to see a list of Users that will be allow or denied. Select Check box for the property sheet. ***Note:*** If enabled, this may prevent the use of Remote Assistance.(NIST)			

Security Options	Multiuser Stand Alone (MUSA)	P2P LAN	client/Server AD
DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDDL) ***Security Objective:*** This policy setting is similar to the **DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL)** setting in that it allows administrators to define additional computer-wide access controls that govern access to all DCOM–based applications on a computer. However, the ACLs that are specified in *this* policy setting control local and remote COM *launch requests* (not access requests) on the computer. The simplest way to think about this access control is as an additional access check call that is done against a computer-wide ACL on each launch of any COM server on the computer. If the access check fails, the call, activation, or launch request will be denied. (This check is in addition to any access check that is run against the server-specific ACLs.) In effect, it provides a minimum authorization standard that must be passed to launch any COM server on the computer. The earlier policy differs in that it provides a minimum access check that is applied to attempts to access an already launched COM server. These computer-wide ACLs provide a way to override weak security settings that are specified by a specific application through CoInitializeSecurity or application-specific security settings. They provide a minimum security standard that must be passed, regardless of the settings of the specific COM server. These ACLs provide a centralized location for an administrator to set general authorization policy that applies to all COM servers on the computer. The **DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDDL)** setting allows you to specify an ACL in two different ways. You can type in the security descriptor in SDDL, or you can choose users and groups and grant or deny them Local Access and Remote Access permissions. Microsoft recommends that you use the built-in user interface to specify the ACL contents that you want to apply with this setting. ***Vulnerability:*** Many COM applications include some security-specific code (for example, to call CoInitializeSecurity) but use weak settings that often allow unauthenticated access to the process. Administrators cannot override these settings to force stronger security in earlier versions of Windows without modification of the application. An attacker could attempt to exploit weak security in an individual application by attacking it through COM calls. Also, COM infrastructure includes the RPCSS, a system service that runs during computer startup and always runs after that. This service manages activation of COM objects and the running object table and provides helper services to DCOM remoting. It exposes RPC interfaces that can be called remotely. Because some COM servers allow unauthenticated remote component activation (as explained in the previous section), these interfaces can be called by anyone, including unauthenticated users. As a result, RPCSS can be attacked by malicious users who use remote, unauthenticated computers. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **Security Options policy** object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. *b.* Select Local Security Setting Tab **DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDDL)** Press Edit Security to see a list of Users that will be allow or denied. Select Check box for the property sheet. Click Okay to complete ***Note:*** If enabled, this may prevent the use of Remote Assistance.(NIST)	Not Defined	Not Defined	Not Defined

Security Options	Multiuser Stand Alone (MUSA)	P2P LAN	client/Server AD
Devices: Allow undock without having to log on ***Security Objective:*** This policy setting determines whether a user must log on to request permission to remove a portable computer from a docking station. If you enable this policy setting, users will be able to press a docked portable computer's physical eject button to safely undock the computer. If you disable this policy setting, the user must log on to receive permission to undock the computer. Only users who have the **Remove Computer from Docking Station** privilege can obtain this permission. **Note**: You should only disable this policy setting for portable computers that cannot be mechanically undocked. Computers that can be mechanically undocked can be physically removed by the user whether or not they use the Windows undocking functionality. The possible values for the **Devices: Allow undock without having to log on** setting are: • Enabled • Disabled • Not Defined ***Vulnerability:*** If this policy setting is enabled, anyone with physical access to portable computers in their docking station could remove them and possibly tamper with them. For computers that do not have docking stations, this policy setting will have no impact. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **Security Options policy** object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. *b.* Select Local Security Setting Tab of **Devices: Allow undock without having to log policy** to set the options. ***Note:*** This setting only pertains to controlled undocking, where appropriate services are stopped When the machine is undocked. There is nothing to prevent an attacker from simply ejecting the machine out of the docking station without doing a graceful disconnect. HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\ undockWithoutLogon = 0	Disabled	Disabled	Disabled

Security Options	Multiuser Stand Alone (MUSA)	P2P LAN	client/Server AD
Devices: Allowed to format and eject removable media ***Security Objective:*** This policy setting determines who is allowed to format and eject removable media. The possible values for the **Devices: Allowed to format and eject removable media** setting are: • Administrators • Administrators and Power Users • Administrators and Interactive Users • Not Defined ***Vulnerability:*** Users may be able to move data on removable disks to a different computer where they have administrative privileges. The user could then take ownership of any file, grant themselves full control and view or modify any file. The fact that most removable storage devices will eject media by pressing a mechanical button diminishes the advantage of this policy setting. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **Security Options policy** object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. *b.* Select Local Security Setting Tab of **Devices: Allowed to format and eject removable media** policy to set the options. Select Administrators from the drop down list ***Note:*** HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ AllocateDASD = 0 (NSA)	Administrators	Administrators	Administrators

Security Options	Multiuser Stand Alone (MUSA)	P2P LAN	client/Server AD
Devices: Prevent users from installing printer drivers ***Security Objective:*** For a computer to print to a network printer, that network printer driver must be installed on the local computer. The **Devices: Prevent users from installing printer drivers** setting determines who can install a printer driver as part of adding a network printer. If you enable this policy setting, only members of the **Administrators** and **Power Users** groups are allowed to install a printer driver when they add a network printer. If you disable this policy setting, any user can install printer drivers when they add a network printer. This policy setting prevents typical users from downloading and installing untrusted printer drivers. **Note**: This policy setting has no impact if an administrator has configured a trusted path to download drivers. If you use trusted paths, the print subsystem attempts to use the trusted path to download the driver. If the trusted path download succeeds, the driver is installed on behalf of any user. If the trusted path download fails, the driver is not installed and the network printer is not added. The possible values for the **Devices: Prevent users from installing printer drivers** setting are: • Enabled • Disabled • Not Defined ***Vulnerability:*** It may be appropriate in some organizations to allow users to install printer drivers on their own workstations. However, you should not allow users to do so on servers. Printer driver installation on a server may unintentionally cause the computer to become less stable. Only Administrators should have this privilege on servers. A malicious user could install inappropriate printer drivers in a deliberate attempt to damage the computer, or a user might accidentally install malicious code that masquerades as a printer driver. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **Security Options policy** object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. *b.* Select Local Security Setting Tab of **Devices: Prevent users from installing printer drivers** policy to set the options. ***NOTE:*** If the printer driver already exists on the local machine, users can add network printers even with this setting enabled. HKLM\System\CurrentControlSet\Control\Print\Providers\LanMan Print Services\Servers\AddPrinterDrivers = 1	Enabled	Enabled	Enabled

Security Options	Multiuser Stand Alone (MUSA)	P2P LAN	client/Server AD
Devices: Restrict CD-ROM access to locally logged-on user only ***Security Objective:*** This policy setting determines whether a CD-ROM is accessible to both local and remote users simultaneously. If you enable this policy setting, only the interactively logged-on user is allowed to access removable CD-ROM media. If this policy setting is enabled and no one is logged on interactively, the CD-ROM can be accessed over the network. The possible values for the **Devices: Restrict CD-ROM access to locally logged-on user only** setting are: • Enabled • Disabled • Not Defined *Vulnerability:* A remote user could potentially access a mounted CD-ROM that contains sensitive information. This risk is small, because CD-ROM drives are not automatically made available as network shares; administrators must deliberately choose to share the drive. However, administrators may wish to deny network users the ability to view data or run applications from removable media on the server. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **Security Options policy** object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. *b.* Select Local Security Setting Tab of **Devices: Restrict CD-ROM access to locally logged-on user only** policy to set the options. ***Note:*** HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateCDRoms = 1 (NSA)	Enabled	Enabled	Enabled

Security Options	Multiuser Stand Alone (MUSA)	P2P LAN	client/Server AD
Devices: Restrict floppy access to locally logged-on user only ***Security Objective:*** This policy setting determines whether removable floppy media are accessible to both local and remote users simultaneously. If you enable this policy setting, only the interactively logged-on user is allowed to access removable floppy media. If this policy setting is enabled and no one is logged on interactively, the floppy can be accessed over the network. The possible values for the **Devices: Restrict floppy access to locally logged-on user only** setting are: • Enabled • Disabled • Not Defined ***Vulnerability:*** A remote user could potentially access a mounted floppy that contains sensitive information. This risk is small because floppy drives are not automatically made available as network shares; administrators must deliberately choose to share the drive. However, administrators may wish to deny network users the ability to view data or run applications from removable media on the server. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **Security Options policy** object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. *b.* Select Local Security Setting Tab of **Devices: Restrict floppy access to locally logged-on user only** policy to set the options. ***Note:*** HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateFloppies = 1 (NSA)	Enabled	Enabled	Enabled

Security Options	Multiuser Stand Alone (MUSA)	P2P LAN	client/Server AD
Devices: Unsigned driver installation behavior ***Security Objective:*** This policy setting determines what happens when an attempt is made to install a device driver that has not been certified and signed by the Windows Hardware Quality Lab (WHQL) by means of the Setup application programming interface (API). The possible values for the **Devices: Unsigned driver installation behavior** setting are: • Silently succeed • Warn but allow installation • Do not allow installation • Not Defined ***Vulnerability:*** This policy setting prevents the installation of unsigned drivers, or warns the administrator that unsigned driver software is about to be installed. This capability can prevent use of the Setup API to install drivers that have not been certified to run on Windows XP or Windows Server 2003. This policy setting will not prevent a method that is used by some attack tools in which malicious .sys files are copied and registered to start as system services. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **Security Options policy** object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. *b.* Select Local Security Setting Tab of **Devices: Unsigned driver installation behavior** policy to set the options. Select Warn but allowed from the drop down list. ***Note:*** HKLM\Software\Microsoft\Driver Signing\Policy = 1(NSA)	Warn but allow installation	Warn but allow installation	Warn but allow installation

Security Options	Multiuser Stand Alone (MUSA)	P2P LAN	client/Server AD
Domain controller: Allow server operators to schedule tasks ***Security Objective:*** This policy setting determines whether server operators are allowed to submit jobs by means of the AT schedule facility. **Note**: This security option setting only affects the AT schedule facility. It does not affect the Task Scheduler facility. The possible values for the **Domain controller: Allow server operators to schedule tasks** setting are: • Enabled • Disabled • Not Defined ***Vulnerability:*** If you enable this policy setting, jobs that are created by server operators by means of the AT service will execute in the context of the account that runs that service. By default, that is the local SYSTEM account. If you enable this policy setting, server operators could perform tasks that SYSTEM is able to do but that they would typically not be able to do, such as add their account to the local **Administrators** group. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **Security Options policy** object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. *b.* Select Local Security Setting Tab of **Domain controller: Allow server operators to schedule tasks** policy to set the options. ***Note:*** This setting is undefined on workstations. (NSA)	Disabled	Disabled	Disabled

Security Options	Multiuser Stand Alone (MUSA)	P2P LAN	client/Server AD
Domain controller: LDAP server signing requirements ***Security Objective:*** This policy setting determines whether the Lightweight Directory Access Protocol (LDAP) server requires LDAP clients to negotiate data signing. The possible values for the **Domain controller: LDAP server signing requirements** setting are: • **None**. Data signatures are not required to bind with the server. If the client requests data signing, the server supports it. • **Require signature**. The LDAP data-signing option must be negotiated unless Transport Layer Security/Secure Socket Layer (TLS/SSL) is in use. • **Not Defined**. ***Vulnerability:*** Unsigned network traffic is susceptible to man-in-the-middle attacks. In such attacks, an intruder captures packets between the server and the client, modifies them, and then forwards them to the client. Where LDAP servers are concerned, an attacker could cause a client to make decisions that are based on false records from the LDAP directory. To lower the risk of such an intrusion in an organization's network, you can implement strong physical security measures to protect the network infrastructure. Also, you could implement Internet Protocol security (IPsec) authentication header mode (AH), which performs mutual authentication and packet integrity for IP traffic to make all types of man-in-the-middle attacks extremely difficult. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **Security Options policy** object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. *b.* Select Local Security Setting Tab of **Domain controller: LDAP server signing requirements** policy to set the options. ***Note:*** This setting is undefined on workstations. (NSA)	Require Signature (unless TSL/SSL are used)	Require Signature (unless TSL/SSL are used)	Require Signature (unless TSL/SSL are used)

Security Options	Multiuser Stand Alone (MUSA)	P2P LAN	client/Server AD
Domain controller: Refuse machine account password changes ***Security Objective:*** This policy setting determines whether or not a domain controller will accept password change requests for computer accounts. The possible values for the **Domain controller: Refuse machine account password changes** setting are: • Enabled • Disabled • Not Defined ***Vulnerability:*** If you enable this policy setting on all domain controllers in a domain, domain members will not be able to change their computer account passwords, and those passwords will be more susceptible to attack. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **Security Options policy** object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. *b.* Select Local Security Setting Tab of **Domain controller: Refuse machine account password changes** policy to set the options. ***Note:*** This setting is undefined on workstations. (NSA)	Disabled	Disabled	Disabled

Security Options	Multiuser Stand Alone (MUSA)	P2P LAN	client/Server AD
Domain member: Digitally encrypt or sign secure channel data (always) ***Security Objective:*** The following policy settings determine whether a secure channel can be established with a domain controller that cannot sign or encrypt secure channel traffic: • **Domain member: Digitally encrypt or sign secure channel data (always)** • **Domain member: Digitally encrypt secure channel data (when possible)** • **Domain member: Digitally sign secure channel data (when possible)** If you enable the **Domain member: Digitally encrypt or sign secure channel data (always)** setting, a secure channel cannot be established with any domain controller that cannot sign or encrypt all secure channel data. To protect authentication traffic from man-in-the-middle, replay, and other types of network attacks, Windows–based computers create a communication channel through NetLogon called Secure Channels. These channels authenticate computer accounts, and they also authenticate user accounts when a remote user connects to a network resource and the user account exists in a trusted domain. This authentication is called pass-through authentication, and it allows a computer that has joined a domain to have access to the user account database in its domain and in any trusted domains. If you enable the **Domain member: Digitally encrypt or sign secure channel data (always)** setting, the **Domain member: Digitally sign secure channel data (when possible)** setting is automatically enabled. The possible values for this policy setting are: • Enabled • Disabled • Not Defined ***Vulnerability:*** When a Windows Server 2003, Windows XP, Windows 2000, or Windows NT computer joins a domain, a computer account is created. After it joins the domain, the computer uses the password for that account to create a secure channel with the domain controller for its domain every time that it restarts. Requests that are sent on the secure channel are authenticated—and sensitive information such as passwords are encrypted—but the channel is not integrity-checked, and not all information is encrypted. If a computer is configured to *always* encrypt or sign secure channel data but the domain controller cannot sign or encrypt any portion of the secure channel data, the computer and domain controller cannot establish a secure channel. 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. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy->Local Policy a. Double click on the **Security Options policy** object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. *b.* Select Local Security Setting Tab of **Domain controller: Refuse machine account password changes** policy to set the options. ***Note***: To enable the **Domain member: Digitally encrypt or sign secure channel data (always)** setting on a member workstation or server, all domain controllers in the domain that the member belongs to must be able to sign or encrypt all secure channel data. This requirement means that all such domain controllers must run Windows NT 4.0 with Service Pack 6a or a later version of the Windows operating system. If this policy is enabled, the policy Domain member: Digitally sign secure channel data (when possible) is automatically enabled. HKLM\System\CurrentControlSet\Services\Netlogon\Parameters\RequireSignOrSeal	Enabled	Enabled	Enabled

Security Options	Multiuser Stand Alone (MUSA)	P2P LAN	client/Server AD
Domain member: Disable machine account password changes ***Security Objective:*** This policy setting determines whether a domain member periodically changes its computer account password. If you enable this policy setting, the domain member cannot change its computer account password. If you disable this policy setting, the domain member is allowed to change its computer account password as specified by the **Domain Member: Maximum age for computer account password** setting, which is every 30 days by default. **Caution**: Do not enable this policy setting. Computer account passwords are used to establish secure channel communications between members and domain controllers and, within the domain, between the domain controllers themselves. After such communications are established, the secure channel transmits sensitive information that is needed to make authentication and authorization decisions. Do not use this policy setting in an attempt to support dual-boot scenarios that use the same computer account. If you want to support such a scenario for two installations that are joined to the same domain, use different computer names for the two installations. This policy setting was added to Windows to make it easier for organizations that stockpile pre-built computers that are put into production months later. It eliminates the need for those computers to rejoin the domain. This policy setting is also sometimes used with imaged computers or those with hardware or software level change prevention. Correct imaging procedures make use of this policy unnecessary for imaged computers. The possible values for the **Domain member: Disable machine account password changes** setting are: • Enabled • Disabled • Not Defined ***Vulnerability:*** The default configuration for Windows Server 2003–based computers that belong to a domain is that they are automatically required to change the passwords for their accounts every 30 days. If you disable this policy setting, computers that run Windows Server 2003 will retain the same passwords as their computer accounts. Computers that are no longer able to automatically change their account password are at risk from an attacker who could determine the password for the computer's domain account. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **Security Options policy** object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. *b.* Select Local Security Setting Tab of **Domain member: Disable machine account password changes** policy to set the options. **Note:** This setting is undefined on workstations. (NSA) HKLM\System\CurrentControlSet\Services\Netlogon\Parameters\SealSecureChannel = 1	Disabled	Disabled	Disabled

Security Options	Multiuser Stand Alone (MUSA)	P2P LAN	client/Server AD
Domain member: Maximum machine account password age ***Security Objective:*** This policy setting determines the maximum allowable age for a computer account password. This setting also applies to Windows 2000 computers, but it is not available through the Security Configuration Manager tools on these computers. The possible values for the **Domain member: Maximum machine account password age** setting are: • A user-defined number of days between 0 and 999 • Not Defined ***Vulnerability*:** In Active Directory–based domains, each computer has an account and password just like every user. By default, the domain members automatically change their domain password every 30 days. If you increase this interval significantly, or set it to 0 so that the computers no longer change their passwords, an attacker will have more time to undertake a brute force attack to guess the password of one or more computer accounts. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **Security Options policy** object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. *b.* Select Local Security Setting Tab of **Domain member: Maximum machine account password age** policy to set the options. ***Note:*** HKLM\System\CurrentControlSet\Services\Netlogon\Parameters\MaximumPasswordAge=7	30 Days	30 Days	30 Days

Security Options	Multiuser Stand Alone (MUSA)	P2P LAN	client/Server AD
Interactive logon: Do not display last user name ***Security Objective:*** This policy setting determines whether the **Log on to Windows** dialog box displays the name of the last user to log on to the computer. If you enable this policy setting, the name of the last user to successfully log on does not display. If you disable this policy setting, the name of the last user to log on will display. The possible values for the **Interactive logon: Do not display last user name** setting are: • Enabled • Disabled • Not Defined ***Vulnerability:*** An attacker with access to the console (for example, someone with physical access or someone who is able to connect to the server through Terminal Services) could view the name of the last user who logged on to the server. The attacker could then try to guess the password, use a dictionary, or use a brute-force attack to try and log on. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **Security Options policy** object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. *b.* Select Local Security Setting Tab of **Interactive logon: Do not display last user name** policy to set the options. *Note:* HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\DontDisplayLastUserName=1	Enabled	Enabled	Enabled

Security Options	Multiuser Stand Alone (MUSA)	P2P LAN	client/Server AD
Domain member: Require strong (Windows 2000 or later) session key ***Security Objective:*** This policy setting determines whether a secure channel can be established with a domain controller that cannot encrypt secure channel traffic with a strong, 128-bit, session key. If you enable this policy setting, a secure channel cannot be established with any domain controller that cannot encrypt secure channel data with a strong key. If you disable this policy setting, 64-bit session keys are allowed. The possible values for the **Domain member: Require strong (Windows 2000 or later) session key** setting are: • Enabled • Disabled • Not Defined ***Vulnerability:*** Session keys that are used to establish secure channel communications between domain controllers and member computers are much stronger in Windows 2000 than they were in previous Microsoft operating systems. Whenever possible, you should take advantage of these stronger session keys to help protect secure channel communications from attacks that attempt to hijack network sessions and eavesdropping. (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 be redirected.) ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **Security Options policy** object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. *b.* Select Local Security Setting Tab of **Domain member: Require strong (Windows 2000 or later) session key** policy to set the options. ***Note:*** To enable this policy setting on a member workstation or server, all domain controllers in the domain to which the member belongs must be able to encrypt secure channel data with a strong, 128-bit key. In other words, all such domain controllers must run Windows 2000 or a later version of the Windows operating system. HKLM\System\CurrentControlSet\Services\Netlogon\Parameters\ RequireStrongKey=1	Enabled	Enabled	Enabled

Security Options	Multiuser Stand Alone (MUSA)	P2P LAN	client/Server AD
Interactive logon: Do not require CTRL+ALT+DEL ***Security Objective:*** This policy setting determines whether users must press CTRL+ALT+DEL before they log on. If you enable this policy setting, users can log on without this key combination. If you disable this policy setting, users must press CTRL+ALT+DEL before they log on to Windows unless they use a smart card for Windows logon. A smart card is a tamper-proof device that stores security information. The possible values for the **Interactive logon: Do not require CTRL+ALT+DEL** setting are: • Enabled • Disabled • Not Defined ***Vulnerability:*** Microsoft developed this feature to make it easier for users with certain types of physical impairments to log on to computers that run Windows. If users are not required to press CTRL+ALT+DEL, they are susceptible to attacks that attempt to intercept their passwords. If CTRL+ALT+DEL is required before logon, user passwords are communicated by means of a trusted path. An attacker could install a Trojan horse program that looks like the standard Windows logon dialog box and capture 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. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **Security Options policy** object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. *b.* Select Local Security Setting Tab of **Interactive logon: Do not require CTRL+ALT+DEL** policy to set the options. ***Note:*** HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableCAD = 0	Disabled	Disabled	Disabled

Security Options	Multiuser Stand Alone (MUSA)	P2P LAN	client/Server AD
Interactive logon: Message text for users attempting to log on ***Security Objective:*** The **Interactive logon: Message text for users attempting to log on** and the **Interactive logon: Message title for users attempting to log on** settings are closely related. The first policy setting specifies a text message that displays to users when they log on, and the second policy setting specifies a title that displays in the title bar of the window that contains the text message. Many organizations use this text for legal purposes; for example, to warn users about the ramifications of misuse of company information, or to warn them that their actions may be audited. The possible values for these policy settings are: • User-defined text • Not Defined ***Vulnerability:*** Displaying a warning message before logon may help prevent an attack by warning the attacker of their misconduct before it happens. It may also help to reinforce corporate policy by notifying employees of the appropriate policy during the logon process. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **Security Options policy** object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. *b.* Select Local Security Setting Tab of **Interactive logon: Message text for users attempting to log** on field to add text messages. **Caution**: Windows XP Professional adds support for logon banners that can exceed 512 characters in length and that can also contain carriage-return line-feed sequences. However, Windows 2000 clients cannot interpret and display these messages. You must use a Windows 2000 computer to create a logon message policy that applies to Windows 2000 computers. If you inadvertently create a logon message policy on a Windows XP Professional computer and you discover that it does not display properly on Windows 2000 computers, do the following: • Reconfigure the setting to **Not Defined**. • Reconfigure the setting using a Windows 2000 computer. You cannot simply change a Windows XP Professional-defined logon message setting on a Windows 2000 computer. You must first reconfigure the setting to **Not Defined**. HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\ LegalNoticeText=”DoD Warning Banner Messages”	Configured with DoD Warning Banner	Configured with DoD Warning Banner	Configured with DoD Warning Banner

Security Options	Multiuser Stand Alone (MUSA)	P2P LAN	client/Server AD
Interactive logon: Message Title for users attempting to log on ***Security Objective:*** Used in conjunction with the logon text, systems should also display a warning statement on the title bar. ***Vulnerability:*** Displaying a warning message before logon may help prevent an attack by warning the attacker of their misconduct before it happens. It may also help to reinforce corporate policy by notifying employees of the appropriate policy during the logon process. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **Security Options policy** object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. *b.* Select Local Security Setting Tab of **Interactive logon: Message title for users attempting to log** on field to add text messages. HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeCaption="Caption of your choice to be displayed on the title bar"	Configured with DoD Warning Banner	Configured with DoD Warning Banner	Configured with DoD Warning Banner

Security Options	Multiuser Stand Alone (MUSA)	P2P LAN	client/Server AD
Interactive logon: Number of previous logons to cache (in case domain controller is not available)	0	0	0
Security Objective: This policy setting determines the number of different unique users who can log on to a Windows domain by using cached account information. Logon information for domain accounts can be cached locally so that if a domain controller cannot be contacted on subsequent logons, a user can still log on. This policy setting determines the number of unique users whose logon information is cached locally. If a domain controller is unavailable and a user's logon information is cached, the user is prompted with the following message: A domain controller for your domain could not be contacted. You have been logged on using cached account information. Changes to your profile since you last logged on may not be available. If a domain controller is unavailable and a user's logon information is not cached, the user is prompted with this message: The system cannot log you on now because the domain <*DOMAIN_NAME*> is not available. The possible values for the **Interactive logon: Number of previous logons to cache (in case domain controller is not available)** setting are: • A user-defined number between 0 and 50 • Not Defined ***Vulnerability:*** The number that is assigned to this policy setting indicates the number of users whose logon information the servers will cache locally. If the number is set to 10, then the server caches logon information for 10 users. When an eleventh user logs on to the computer, the server overwrites the oldest cached logon session. 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 attempt to determine user passwords. To mitigate this type of attack, Windows encrypts the information and obscures its physical location. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **Security Options policy** object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. *b.* Select Local Security Setting Tab of **Interactive logon: Number of previous logons to cache (in case domain controller is not available)** policy to set the options. Enter the number 0 for the count. ***Note:*** HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CachedLogonsCount=0			

Security Options	Multiuser Stand Alone (MUSA)	P2P LAN	client/Server AD
Interactive logon: Prompt user to change password before expiration ***Security Objective:*** This policy setting determines how many days in advance users are warned that their password is about to expire. With this advance warning, the user has time to construct a password that is sufficiently strong. The possible values for the **Interactive logon: Prompt user to change password before expiration** setting are: • User defined number of days between 1 and 999 • Not Defined ***Vulnerability:*** Microsoft recommends 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 be locked out of the computer when their passwords expire. This condition could lead to confusion for users who access the network locally, or make it impossible for users to access your organization's network through dial-up or virtual private network (VPN) connections. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **Security Options policy** object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. *b.* Select Local Security Setting Tab of **Interactive logon: Prompt user to change password before expiration** on field to set option. Enter 14 into the combo box. ***Note:*** HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\PasswordExpiryWarning=14	14	14	14

Security Options	Multiuser Stand Alone (MUSA)	P2P LAN	client/Server AD
Interactive logon: Require Domain Controller authentication to unlock workstation ***Security Objective:*** Logon information is required to unlock a locked computer. For domain accounts, the **Interactive logon: Require Domain Controller authentication to unlock workstation** setting determines whether it is necessary to contact a domain controller to unlock a computer. If you enable this setting, a domain controller must authenticate the domain account that is being used to unlock the computer. If you disable this setting, logon information confirmation with a domain controller is not required for a user to unlock the computer. However, if you configure the **Interactive logon: Number of previous logons to cache (in case domain controller is not available)** setting to a value that is greater than zero, then the user's cached credentials will be used to unlock the computer. **Note**: This setting applies to Windows 2000 computers, but it is not available through the Security Configuration Manager tools on these computers. The possible values for the **Interactive logon: Require Domain Controller authentication to unlock workstation** setting are: • Enabled • Disabled • Not Defined ***Vulnerability*** By default, the computer caches in memory the credentials of any users who are authenticated locally. The computer uses these cached credentials to authenticate anyone who attempts to unlock the console. 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 after the account is authenticated. User privileges are not updated, and (more importantly) disabled accounts are still able to unlock the console of the computer. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **Security Options policy** object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. *b.* Select Local Security Setting Tab of **Interactive logon: Require Domain Controller authentication to unlock workstation** policy to set options. ***Note:*** HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ForceUnlockLogon=1	Not Defined	Not Defined	Enabled

Security Options	Multiuser Stand Alone (MUSA)	P2P LAN	client/Server AD
Interactive logon: Require smart card (Note: Only enable this setting if a smart card solution is employed) **Security Objective:** This policy setting requires users to log on to a computer with a smart card. **Note**: This setting applies to Windows 2000 computers, but it is not available through the Security Configuration Manager tools on these computers. The possible values for the **Interactive logon: Require smart card** setting are: • Enabled • Disabled • Not Defined **Vulnerability:** Requirements to use long, complex passwords for authentication enhance network security, especially if the users must change their passwords regularly. This approach reduces the chance that an attacker will be able to guess a user's password by means of a brute force attack. However, it is difficult to make users choose strong passwords, and even strong passwords are vulnerable to brute-force attacks if an attacker has sufficient time and computing resources. The use of smart cards instead of passwords for authentication dramatically increases security, because current technology makes it almost impossible for an attacker to impersonate another user. Smart cards that require personal identification numbers (PINs) provide two-factor authentication. In other words, the user must both possess the smart card and know its PIN. An attacker who captures the authentication traffic between the user's computer and the domain controller will find it extremely difficult to decrypt the traffic and, even if they do, the next time the user logs onto the network a new session key will be generated to encrypt traffic between the user and the domain controller. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **Security Options policy** object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. *b.* Select Local Security Setting Tab of **Interactive logon: Require smart card** policy to set options. ***Note:*** HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\ScRemoveOption=1	Enabled	Enabled	Enabled

Security Options	Multiuser Stand Alone (MUSA)	P2P LAN	client/Server AD
Interactive logon: Smart card removal behavior ***Security Objective:*** This policy setting determines what happens when the smart card for a logged-on user is removed from the smart card reader. The possible values for the **Interactive logon: Smart card removal behavior** setting are: • No Action • Lock Workstation • Force Logoff • Not Defined ***Vulnerability:*** If smart cards are used for authentication, then the computer should automatically lock itself when the card is removed. This approach will prevent malicious users from accessing the computers of users who forget to manually lock their workstations when they are away from them. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **Security Options policy** object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. *b.* Select Local Security Setting Tab of **Interactive logon: Smart card removal behavior** policy to set options. ***Note:*** HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ScRemoveOption=1	Lock Workstation	Lock Workstation	Lock Workstation

Security Options	Multiuser Stand Alone (MUSA)	P2P LAN	client/Server AD
Microsoft Network Client: Digitally Sign Communications (Always) ***Security Objective:*** When enabled, this setting forces SMB clients to always digitally sign SMB communications. Digitally signing SMB communications closes "man-in-the-middle" attacks and supports message authentication, which prevents active message attacks. (NSA) The possible values for settings are: • Enabled • Disabled • Not Defined ***Vulnerability:*** Implementation of digital signatures in high security networks helps to prevent the impersonation of clients and servers. This type of impersonation is known as session hijacking, and uses tools that allow attackers who have access to the same network as the client or server to interrupt, end, or steal a session in progress. Attackers can potentially intercept and modify unsigned SMB packets and then modify the traffic and forward it so that the server might perform undesirable actions. Alternatively, the attacker could pose as the server or client after legitimate authentication and gain unauthorized access to data. SMB is the resource sharing protocol that is supported by many Microsoft operating systems. It is the basis of NetBIOS and many other protocols. SMB signatures authenticate both users and the servers that host the data. If either side fails the authentication process, data transmission will not take place. **Note**: An alternative countermeasure that could protect all network traffic would be to implement digital signatures with IPsec. There are hardware-based accelerators for IPsec encryption and signing that could be used to minimize the performance impact on the servers' CPUs. No such accelerators are available for SMB signing. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **Security Options policy** object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. **b.** Select Local Security Setting Tab of **Microsoft Network Client: Digitally Sign Communications (Always)** policy to set options. ***Note:*** HKLM\System\CurrentControlSet\Services\LanmanWorkstation\ Parameters\ RequireSecuritySignature\HKLM\System\CurrentControlSet\Services\ LanmanWorkstation\Parameters\EnableSecuritySignature=1	Enabled	Enabled	Enabled

Security Options	Multiuser Stand Alone (MUSA)	P2P LAN	client/Server AD
Microsoft Network Client: Digitally Sign Communications (If Server Agrees)	Enabled	Enabled	Enabled
Security Objective: There are four separate settings that relate to digital signatures for Server Message Block (SMB) communications: • **Microsoft Network Client: Digitally Sign Communications (Always)** • **Microsoft Network Server: Digitally Sign Communications (Always)** • **Microsoft Network Client: Digitally Sign Communications (If Server Agrees)** • **Microsoft Network Server: Digitally Sign Communications (If Client Agrees)** The possible values for each of these policy settings are: • Enabled • Disabled • Not Defined			
Vulnerability: Implementation of digital signatures in high security networks helps to prevent the impersonation of clients and servers. This type of impersonation is known as session hijacking, and uses tools that allow attackers who have access to the same network as the client or server to interrupt, end, or steal a session in progress. Attackers can potentially intercept and modify unsigned SMB packets and then modify the traffic and forward it so that the server might perform undesirable actions. Alternatively, the attacker could pose as the server or client after legitimate authentication and gain unauthorized access to data. SMB is the resource sharing protocol that is supported by many Microsoft operating systems. It is the basis of NetBIOS and many other protocols. SMB signatures authenticate both users and the servers that host the data. If either side fails the authentication process, data transmission will not take place.			
Procedure: Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **Security Options policy** object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. **b.** Select Local Security Setting Tab of **Microsoft Network Client: Digitally Sign Communications (If Server Agrees)** policy to set options.			
Note: An alternative countermeasure that could protect all network traffic would be to implement digital signatures with IPsec. There are hardware-based accelerators for IPsec encryption and signing that could be used to minimize the performance impact on the servers' CPUs. No such accelerators are available for SMB signing. HKLM\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnableSecuritySignature=1			

Security Options	Multiuser Stand Alone (MUSA)	P2P LAN	client/Server AD
Microsoft network client: Send unencrypted password to third-party SMB server ***Security Objective:*** This policy setting allows the SMB redirector to send plaintext passwords to non-Microsoft SMB servers that do not support password encryption during authentication. The possible values for the **Microsoft network client: Send unencrypted password to third-party SMB servers** setting are: • Enabled • Disabled • Not Defined ***Vulnerability:*** If you enable this policy setting, the server can transmit passwords in plaintext across the network to other computers that offer SMB services. These other computers may not use any of the SMB security mechanisms that are included with Windows Server 2003. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **Security Options policy** object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. *b.* Select Local Security Setting Tab of **Microsoft network client: Send unencrypted password to third-party SMB server** policy to set options. ***Note:*** Enabling this will allow unencrypted (plain text) passwords to be sent across the network when authenticating to an SMB server that requests this option. This reduces the overall security of an environment and should only be done after careful consideration of the consequences of plain text passwords in your specific environment. HKLM\System\CurrentControlSet\Services\LanmanWorkstation\ Parameters\EnablePlainTextPassword=0	Disabled	Disabled	Disabled

Security Options	Multiuser Stand Alone (MUSA)	P2P LAN	client/Server AD
Microsoft network server: Amount of idle time required before suspending session ***Security Objective:*** This policy setting determines the amount of continuous idle time that must pass in a SMB session before the session is suspended because of inactivity. Administrators can use this policy setting to control when a computer suspends an inactive SMB session. The session automatically re-establishes when client activity resumes. A value of **0** will disconnect an idle session as quickly as possible. The maximum value is 99999, which is 208 days; in effect, this value disables the setting. The possible values for the **Microsoft network server: Amount of idle time required before suspending session** setting are: • User-defined period of time in minutes • Not Defined ***Vulnerability:*** Each SMB session consumes server resources, and numerous null sessions will slow the server or possibly cause it to fail. An attacker could repeatedly establish SMB sessions until the server's SMB services become slow or unresponsive. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **Security Options policy** object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. **b.** Select Local Security Setting Tab of **Microsoft network server: Amount of idle time required before suspending session policy** to set options. ***Note:*** HKLM\System\CurrentControlSet\Services\LanManServer\Parameters\ AutoDisconnect=15	15	15	15

Security Options	Multiuser Stand Alone (MUSA)	P2P LAN	client/Server AD
Microsoft Network Server: Digitally Sign Communications (Always) ***Security Objective:*** The digital signatures for Server Message Block (SMB) communications: **Microsoft Network Server: Digitally Sign Communications (Always)** Determines if the SMB server is required to perform SMB packet signing. (NSA) The possible values for each of these policy settings are: • Enabled • Disabled • Not Defined ***Vulnerability:*** Implementation of digital signatures in high security networks helps to prevent the impersonation of clients and servers. This type of impersonation is known as session hijacking, and uses tools that allow attackers who have access to the same network as the client or server to interrupt, end, or steal a session in progress. Attackers can potentially intercept and modify unsigned SMB packets and then modify the traffic and forward it so that the server might perform undesirable actions. Alternatively, the attacker could pose as the server or client after legitimate authentication and gain unauthorized access to data. SMB is the resource sharing protocol that is supported by many Microsoft operating systems. It is the basis of NetBIOS and many other protocols. SMB signatures authenticate both users and the servers that host the data. If either side fails the authentication process, data transmission will not take place. **Note**: An alternative countermeasure that could protect all network traffic would be to implement digital signatures with IPsec. There are hardware-based accelerators for IPsec encryption and signing that could be used to minimize the performance impact on the servers' CPUs. No such accelerators are available for SMB signing. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies c. Double click on the **Security Options policy** object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. **d.** Select Local Security Setting Tab of **Microsoft Network Server: Digitally Sign Communications (Always)** policy to set options. ***Note:*** HKLM\System\CurrentControlSet\Services\LanmanWorkstation\ Parameters\RequireSecuritySignature HKLM\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnableSecuritySignature=1	Enabled	Enabled	Enabled

Security Options	Multiuser Stand Alone (MUSA)	P2P LAN	client/Server AD
Microsoft Network Server: Digitally Sign Communications (If Client Agrees) ***Security Objective:*** There are settings that relate to digital signatures for Server Message Block (SMB) communications for **Microsoft Network Server: Digitally Sign Communications (If Client Agrees)** The possible values for each of these policy settings are: • Enabled • Disabled • Not Defined ***Vulnerability:*** Implementation of digital signatures in high security networks helps to prevent the impersonation of clients and servers. This type of impersonation is known as session hijacking, and uses tools that allow attackers who have access to the same network as the client or server to interrupt, end, or steal a session in progress. Attackers can potentially intercept and modify unsigned SMB packets and then modify the traffic and forward it so that the server might perform undesirable actions. Alternatively, the attacker could pose as the server or client after legitimate authentication and gain unauthorized access to data. SMB is the resource sharing protocol that is supported by many Microsoft operating systems. It is the basis of NetBIOS and many other protocols. SMB signatures authenticate both users and the servers that host the data. If either side fails the authentication process, data transmission will not take place. **Note**: An alternative countermeasure that could protect all network traffic would be to implement digital signatures with IPsec. There are hardware-based accelerators for IPsec encryption and signing that could be used to minimize the performance impact on the servers' CPUs. No such accelerators are available for SMB signing. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **Security Options policy** object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. b. Select Local Security Setting Tab of **Microsoft Network Server: Digitally Sign Communications (If Client Agrees)** policy to set options. ***Note:*** HKLM\System\CurrentControlSet\Services\LanManServer\Parameters\ EnableSecuritySignature=1	Enabled	Enabled	Enabled

Security Options	Multiuser Stand Alone (MUSA)	P2P LAN	client/Server AD
Microsoft network server: Disconnect clients when logon hours expire ***Security Objective:*** This policy setting determines whether to disconnect users who are connected to the local computer outside their user account's valid logon hours. It affects the SMB component. If you enable this policy setting, client sessions with the SMB service will be forcibly disconnected when the client's logon hours expire. If you disable this policy setting, established client sessions will be maintained after the client's logon hours expire. If you enable this policy setting you should also enable **Network security: Force logoff when logon hours expire**. The possible values for the **Microsoft network server: Disconnect clients when logon hours expire** setting are: • Enabled • Disabled • Not Defined ***Vulnerability:*** If your organization configures logon hours for users, then it makes sense to enable this policy setting. Otherwise, users who should not have access to network resources outside of their logon hours may actually be able to continue to use those resources with sessions that were established during allowed hours. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies c. Double click on the **Security Options policy** object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. d. Select Local Security Setting Tab of **Microsoft network server: Disconnect clients when logon hours expire** policy to set options. ***Note:*** HKLM\System\CurrentControlSet\Services\LanManServer\Parameters\ EnableForcedLogoff=1	Enabled	Enabled	Enabled

Security Options	Multiuser Stand Alone (MUSA)	P2P LAN	client/Server AD
Network access: Allow anonymous SID/Name translation ***Security Objective:*** This policy setting determines whether an anonymous user can request SID attributes for another user. The possible values for the **Network access: Allow anonymous SID/Name translation** setting are: • Enabled • Disabled • Not Defined ***Vulnerability:*** If this policy setting is enabled, a user with local access could use the well-known Administrator's SID to learn the real name of the built-in Administrator account, even if it has been renamed. That person could then use the account name to initiate a password guessing attack. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **Security Options policy** object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. b. Select Local Security Setting Tab of **Network access: Allow anonymous SID/Name translation policy** to set options.	Disabled	Disabled	Disabled

Security Options	Multiuser Stand Alone (MUSA)	P2P LAN	client/Server AD
Network access: Do not allow anonymous enumeration of SAM accounts ***Security Objective:*** This policy setting determines what additional permissions will be granted for anonymous connections to the computer. Windows allows anonymous users to perform certain activities, such as enumerate the names of domain accounts and network shares. This capability is convenient, for example, when an administrator wants to grant access to users in a trusted domain that does not maintain a reciprocal trust. However, even if this setting enabled, anonymous users will still have access to any resources that have permissions that explicitly include the special built-in group **ANONYMOUS LOGON**. In Windows 2000, a similar policy setting called **Additional Restrictions for Anonymous Connections** managed a registry value called **RestrictAnonymous**, which was located in the **HKLM\SYSTEM\CurrentControlSet\Control\LSA** registry key. In Windows Server 2003, the policy settings **Network access: Do not allow anonymous enumeration of SAM accounts** and **Network access: Do not allow anonymous enumeration of SAM accounts and shares** replace the Windows 2000 policy setting. They manage the registry values **RestrictAnonymousSAM** and **RestrictAnonymous**, respectively, which are both located in the **HKLM\System\CurrentControlSet\Control\Lsa** registry key. The possible values for the **Network access: Do not allow anonymous enumeration of SAM accounts** setting are: • Enabled • Disabled • Not Defined ***Vulnerability:*** An unauthorized user could anonymously list account names and use the information to perform social engineering attacks or attempt to guess passwords. (Social engineering attacks try to deceive users in some way to obtain passwords or some form of security information.) ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **Security Options policy** object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. b. Select Local Security Setting Tab of **Network access: Do not allow anonymous enumeration policy** to set options. ***Note:*** Do not allow enumeration of SAM accounts. HKLM\System\CurrentControlSet\Control\Lsa\RestrictAnonymousSAM=1	Enabled	Enabled	Enabled

Security Options	Multiuser Stand Alone (MUSA)	P2P LAN	client/Server AD
Network access: Do not allow storage of credentials or .NET Passports for network authentication ***Security Objective:*** This policy setting determines whether the Stored User Names and Passwords feature may save passwords or credentials for later use when it gains domain authentication. If you enable this policy setting, the Stored User Names and Passwords feature of Windows does not store passwords and credentials. The possible values for the **Network access: Do not allow storage of credentials or.NET Passports for network authentication** setting are: • Enabled • Disabled • Not Defined ***Vulnerability:*** Passwords that are cached can be accessed by the user when logged on to the computer. Although this information may sound obvious, a problem can arise if the user unknowingly executes hostile code that reads the passwords and forwards them to another, unauthorized user. ***Note:*** The chances of success for this exploit and others that involve hostile code will be reduced significantly for organizations that effectively implement and manage an enterprise antivirus solution combined with sensible software restriction policies. Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **Security Options policy** object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. b. Select Local Security Setting Tab of **Network access: Do not allow storage of credentials or.NET Passports for network authentication policy** to set options. *Note:* The chances of success for this exploit and others that involve hostile code will be reduced significantly for organizations that effectively implement and manage an enterprise antivirus solution combined with sensible software restriction policies. For more information about software restriction policies. HKLM\System\CurrentControlSet\Control\Lsa\DisableDomainCreds=1	Enabled	Enabled	Enabled

Security Options	Multiuser Stand Alone (MUSA)	P2P LAN	client/Server AD
Network access: Let Everyone permissions apply to anonymous users ***Security Objective:*** This policy setting determines what additional permissions are granted for anonymous connections to the computer. If you enable this policy setting, anonymous users can enumerate the names of domain accounts and network shares and perform certain other activities. This capability is convenient, for example, when an administrator wants to grant access to users in a trusted domain that does not maintain a reciprocal trust. By default, the token that is created for anonymous connections does not include the Everyone SID. Therefore, permissions that are assigned to the **Everyone** group do not apply to anonymous users. If you enable this policy setting, the Everyone SID is added to the token that is created for anonymous connections, and anonymous users will be able to access any resource for which the **Everyone** group has been assigned permissions. The possible values for the **Network access: Let Everyone permissions apply to anonymous users** setting are: • Enabled • Disabled • Not Defined ***Vulnerability:*** An unauthorized user could anonymously list account names and shared resources and use the information to attempt to guess passwords, perform social engineering attacks, or launch DoS attacks. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **Security Options policy** object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. b. Select Local Security Setting Tab of **Network access: Let Everyone permissions apply to anonymous users** policy to set options. ***Note:*** Disabling this option is the equivalent of setting RestrictAnonymous = 2 on Windows 2000. HKLM\System\CurrentControlSet\Control\Lsa\EveryoneIncludesAnonymous=0	Disabled	Disabled	Disabled

Security Options	Multiuser Stand Alone (MUSA)	P2P LAN	client/Server AD
Network access: Named Pipes that can be accessed anonymously ***Security Objective:*** This policy setting determines which communication sessions, or pipes, will have attributes and permissions that allow anonymous access. The possible values for the **Network access: Named Pipes that can be accessed anonymously** setting are: • A user-defined list of shares • Not Defined For this policy setting to take effect, you must also enable the **Network access: Restrict anonymous access to named pipes and shares** setting. ***Vulnerability:*** You can restrict access over named pipes such as COMNAP and LOCATOR to help prevent unauthorized access to the network. The default list of named pipes and their purpose is provided in the following table. **Table 5.1: Default Named Pipes That Are Accessible Anonymously** **Named pipe** — **Purpose** COMNAP — SNABase named pipe. Systems Network Architecture (SNA) is a collection of network protocols that were originally developed for IBM mainframe computers. COMNODE — SNA Server named pipe. SQL\QUERY — Default named pipe for SQL Server. SPOOLSS — Named pipe for the Print Spooler service. EPMAPPER — End Point Mapper named pipe. LOCATOR — Remote Procedure Call Locator service named pipe. TrkWks — Distributed Link Tracking Client named pipe. TrkSvr — Distributed Link Tracking Server named pipe. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy->Local Policy a. Double click on the **Security Options policy** object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. b. Select Local Security Setting Tab of **Network access: Named Pipes that can be accessed anonymously** policy to set options. Do not enter any value in the text field ***Note:*** Pipes are internal communication processes that are identified by ID numbers that vary between systems. To facilitate access, pipes are given names that do not vary among systems. This setting determines which pipes will allow anonymous access. KLM\System\CurrentControlSet\Services\LanManServer\Parameters\NullSessionPipes	Set to Null but No value in the text	Set to Null but No value in the text	Set to Null but No value in the text

Security Options	Multiuser Stand Alone (MUSA)	P2P LAN	client/Server AD
Network access: Remotely accessible registry paths ***Security Objective:*** This policy setting determines which registry paths will be accessible when an application or process references the **WinReg** key to determine access permissions. The possible values for the **Network access: Remotely accessible registry paths** setting are: • A user-defined list of paths • Not Defined ***Vulnerability:*** The registry is a database that contains computer configuration information, and much of the information is sensitive. An attacker could use this information to facilitate unauthorized activities. To reduce the risk of such an attack, suitable ACLs are assigned throughout the registry to help protect it from access by unauthorized users. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **Security Options policy** object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. b. Select Local Security Setting Tab of **Network access: Remotely accessible registry paths** policy to set options. ***Note:*** This setting specifies registry paths that will be accessible from a remote computer. HKLM\System\CurrentControlSet\Control\SecurePipeServers\Winreg\AllowedPaths\Machine (NSA) System\CurrentControlSet\Control\ProductOptions, System\CurrentControlSet\Control\Print\Printers, System\CurrentControlSet\Control\Server Applications, System\CurrentControlSet\Services\Eventlog, Software\Microsoft\OLAP Server, Software\Microsoft\Windows NT\CurrentVersion, System\CurrentControlSet\Control\ContentIndex, System\CurrentControlSet\Control\Terminal Server, System\CurrentControlSet\Control\Terminal Server\UserConfig, System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration (NIST)	Set to Null or enable but no text value	Set to Null or enable but no text value	Set to Null or enable but no text value

Security Options	Multiuser Stand Alone (MUSA)	P2P LAN	client/Server AD
Network access: Remotely accessible registry paths and sub-paths ***Security Objective:*** This policy setting determines which registry paths and sub-paths will be accessible when an application or process references the **WinReg** key to determine access permissions. The possible values for the **Network access: Remotely accessible registry paths and sub-paths** setting are: • A user-defined list of paths • Not Defined ***Vulnerability:*** As stated earlier, the registry contains sensitive computer configuration information that could be used by an attacker to facilitate unauthorized activities. The fact that the default ACLs assigned throughout the registry are fairly restrictive and help to protect the registry from access by unauthorized users reduces the risk of such an attack. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **Security Options policy** object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. b. Select both Success and Failure check box in the **Network access: Remotely accessible registry paths and sub-paths** policy to set options.	Set to Null or enable but no text value	Set to Null or enable but no text value	Set to Null or enable but no text value(add to list as required)

Security Options	Multiuser Stand Alone (MUSA)	P2P LAN	client/Server AD
Network access: Restrict anonymous access to Named Pipes and Shares ***Security Objective:*** When enabled, this policy setting restricts anonymous access to only those shares and pipes that are named in the **Network access: Named pipes that can be accessed anonymously** and **Network access: Shares that can be accessed anonymously** settings. This policy setting controls null session access to shares on your computers by adding **RestrictNullSessAccess** with the value **1** in the registry key **HKLM\System\CurrentControlSet\Services\LanManServer\Parameters**. This registry value toggles null session shares on or off to control whether the server service restricts unauthenticated clients' access to named resources. The possible values for the **Network access: Restrict anonymous access to Named Pipes and Shares** setting are: • Enabled • Disabled • Not Defined ***Vulnerability*** Null sessions are a weakness that can be exploited through shares (including the default shares) on computers in your environment. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **Security Options policy** object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. b. Select Local Security Setting Tab of **Network access: Restrict anonymous access to Named Pipes and Shares** policy to set options.	Enabled	Enabled	Enabled

Security Options	Multiuser Stand Alone (MUSA)	P2P LAN	client/Server AD
Network access: Shares that can be accessed anonymously ***Security Objective:*** This policy setting determines which network shares can be accessed by anonymous users. The possible values for the **Network access: Shares that can be accessed anonymously** setting are: • A user-defined list of shares • Not Defined ***Vulnerability:*** It is very dangerous to enable this setting. Any shares that are listed can be accessed by any network user, which could lead to the exposure or corruption of sensitive data. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **Security Options policy** object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. b. Select Local Security Setting Tab of **Network access: Shares that can be accessed anonymously** policy to set options. ***Note:*** HKLM\System\CurrentControlSet\Services\LanManServer\Parameters\NullSessionShares (NSA)	Set to Null Value	Set to Null Value	Set to Null Value (only if required)

Security Options	Multiuser Stand Alone (MUSA)	P2P LAN	client/Server AD
Network access: Sharing and security model for local accounts ***Security Objective:*** This policy setting determines how network logons that use local accounts are authenticated. If you configure this policy setting to **Classic**, network logons that use local account credentials authenticate with those credentials. If you configure this policy setting to **Guest only**, network logons that use local accounts are automatically mapped to the Guest account. The **Classic** model provides precise control over access to resources, and allows you to grant different types of access to different users for the same resource. Conversely, the **Guest only** model treats all users equally as the Guest user account, and they all receive the same level of access to a given resource, which can be either Read Only or Modify. The default configuration in stand-alone Windows XP Professional is **Guest only**. The default for Windows XP computers that are joined to a domain and Windows Server 2003 computers is **Classic**. When the computer is not joined to a domain, this policy setting also tailors the **Sharing** and **Security** tabs in Windows Explorer to correspond to the sharing and security model that is being used. This setting has no effect on Windows 2000 computers. The possible values for the **Network access: Sharing and security model for local accounts** setting are: • Classic. Local users authenticate as themselves. • Guest only. Local users authenticate as Guest. • Not Defined ***Vulnerability,*** With the **Guest only** model, any user who can authenticate to your computer over the network does so with guest privileges, which probably means that they will not have write access to shared resources on that computer. Although this restriction does increase security, it makes it more difficult for authorized users to access shared resources on those computers because ACLs on those resources must include access control entries (ACEs) for the Guest account. With the **Classic** model, local accounts should be password protected. Otherwise, if Guest access is enabled, anyone can use those user accounts to access shared system resources. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy->Local Policies a. Double click on the **Security Options policy** object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. b. Select Local Security Setting Tab of **Network access: Sharing and security model for local accounts** policy to set options.	Classic-local user authenticate as them selves	Classic-local user authenticate as them selves	Classic-local user authenticate as them selves
Note: This option is set to Classic by default for Windows XP Professional machines joined to a domain. Standalone Windows XP machines set this option to Guest Only by default. Network logons using domain accounts and interactive logons performed by using services such as Telnet or Terminal Services are not affected by this setting. WARNING: The Guest only model allows any user who can access the computer over the network (including anonymous Internet users) the ability to access shared resources. HKLM\System\CurrentControlSet\Control\Lsa\ForceGuest=0			

Security Options	Multiuser Stand Alone (MUSA)	P2P LAN	client/Server AD
Network security: Do not store LAN Manager hash value on next password change ***Security Objective:*** This policy setting determines whether LAN Manager can store hash values for the new password the next time the password is changed. The possible values for the **Network security: Do not store LAN Manager hash value on next password change** setting are: • Enabled • Disabled • Not Defined ***Vulnerability:*** The SAM file can be targeted by attackers who seek access to username and password hashes. Such attacks use special tools to crack passwords, which can then be used to impersonate users and gain access to resources on your network. These types of attacks will not be prevented if you enable this policy setting, but it will be much more difficult for these types of attacks to succeed. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **Security Options policy** object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. b. Select Local Security Setting Tab of **Network security: Do not store LAN Manager hash value on next password change** policy to set options. ***NOTE:*** The LAN Manager hash is used for backwards compatibility with pre-Windows NT machines and some applications. Since it is a hash of the Windows password converted to all uppercase and treated as two 7-character passwords, it is easier to crack and is the primary target in password cracking utilities. For this reason, it is recommended that the LM hash not be stored in the SAM. Enabling this option will result in problems with communications to legacy operating systems or applications that only support LANManager authentication. HKLM\System\CurrentControlSet\Control\Lsa\NoLMHash=1	Enabled	Enabled	Enabled

Security Options	Multiuser Stand Alone (MUSA)	P2P LAN	client/Server AD
Network security: LAN Manager authentication level ***Security Objective:*** LAN Manager (LM) is a family of early Microsoft client/server software that allows users to link personal computers together on a single network. Network capabilities include transparent file and print sharing, user security features, and network administration tools. In Active Directory domains, the Kerberos protocol is the default authentication protocol. However, if the Kerberos protocol is not negotiated for some reason, Active Directory will use LM, NTLM, or NTLMv2. LAN Manager authentication includes the LM, NTLM, and NTLM version 2 (NTLMv2) variants, and is the protocol that is used to authenticate all Windows clients when they perform the following operations: • Join a domain • Authenticate between Active Directory forests • Authenticate to down-level domains • Authenticate to computers that do not run Windows 2000, Windows Server 2003, or Windows XP) • Authenticate to computers that are not in the domain . The possible values for the **Network security: LAN Manager authentication level** setting are: • Send LM & NTLM responses • Send LM & NTLM — use NTLMv2 session security if negotiated • Send NTLM responses only • Send NTLMv2 responses only • Send NTLMv2 responses only\refuse LM • Send NTLMv2 responses only\refuse LM & NTLM • Not Defined *Continued*	Send NTLMv2 response only\refuse LM and NTLM	Send NTLMv2 response only\refuse LM and NTLM	Send NTLMv2 response only\refuse LM and NTLM

Security Options	Multiuser Stand Alone (MUSA)	P2P LAN	client/Server AD
Network security: LAN Manager authentication level **Security Objective:** (Continued) The **Network security: LAN Manager authentication level** setting determines which challenge/response authentication protocol is used for network logons. This choice affects the authentication protocol level that clients use, the session security level that the computers negotiate, and the authentication level that servers accept as follows: • **Send LM & NTLM responses**. Clients use LM and NTLM authentication and never use NTLMv2 session security. Domain controllers accept LM, NTLM, and NTLMv2 authentication. • **Send LM & NTLM – use NTLMv2 session security if negotiated**. Clients use LM and NTLM authentication and use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication. • **Send NTLM response only**. Clients use NTLM authentication only and use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication. • **Send NTLMv2 response only**. Clients use NTLMv2 authentication only and use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication. • **Send NTLMv2 response only\refuse LM**. Clients use NTLMv2 authentication only and use NTLMv2 session security if the server supports it. Domain controllers refuse LM (accept only NTLM and NTLMv2 authentication). • **Send NTLMv2 response only\refuse LM & NTLM**. Clients use NTLMv2 authentication only and use NTLMv2 session security if the server supports it. Domain controllers refuse LM and NTLM (accept only NTLMv2 authentication). These settings correspond to the levels discussed in other Microsoft documents as follows: • **Level 0 – Send LM and NTLM response; never use NTLMv2 session security**. Clients use LM and NTLM authentication, and never use NTLMv2 session security. Domain controllers accept LM, NTLM, and NTLMv2 authentication. • **Level 1 – Use NTLMv2 session security if negotiated**. Clients use LM and NTLM authentication, and use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication. • **Level 2 – Send NTLM response only**. Clients use only NTLM authentication, and use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication. • **Level 3 – Send NTLMv2 response only**. Clients use NTLMv2 authentication, and use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication. • **Level 4 – Domain controllers refuse LM responses**. Clients use NTLM authentication, and use NTLMv2 session security if the server supports it. Domain controllers refuse LM authentication, that is, they accept NTLM and NTLMv2. • **Level 5 – Domain controllers refuse LM and NTLM responses (accept only NTLMv2)**. Clients use NTLMv2 authentication, use and NTLMv2 session security if the server supports it. Domain controllers refuse NTLM and LM authentication (they accept only NTLMv2). *Continued*	Send NTLMv2 response only\refuse LM and NTLM	Send NTLMv2 response only\refuse LM and NTLM	Send NTLMv2 response only\refuse LM and NTLM

Security Options	Multiuser Stand Alone (MUSA)	P2P LAN	client/Server AD
Network security: LAN Manager authentication level ***Vulnerability:*** Windows 2000, Windows Server 2003, and Windows XP clients are configured by default to send LM and NTLM authentication responses (Windows 9x clients only send LM). The default setting on servers allows all clients to authenticate with servers and use their resources. However, this means that LM responses—the weakest form of authentication response—are sent over the network, and it is potentially possible for attackers to sniff that traffic to more easily reproduce the user's password. The Windows 9x and Windows NT operating systems cannot use the Kerberos version 5 protocol for authentication. For this reason, in a Windows Server 2003 domain, these computers authenticate by default with both the LM and NTLM protocols for network authentication. You can enforce a more secure authentication protocol for Windows 9x and Windows NT by using NTLMv2. For the logon process, NTLMv2 uses a secure channel to protect the authentication process. Even if you use NTLMv2 for legacy clients and servers, Windows-based clients and servers that are members of the domain will use the Kerberos authentication protocol to authenticate with Windows Server 2003 domain controllers. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **Security Options policy** object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. b. Select Local Security Setting Tab of **Network security: LAN Manager authentication level** policy to set options. ***Note:*** Some Windows processes, such as Cluster Services, use NTLM to authenticate. Use of the recommended setting may cause these services to fail. For more information on NTLM and Cluster Services, see KB Article Q272129http://support.microsoft.com/default.asp?scid=kb;EN=US;q 272129 Setting this value higher than 2 on a Windows XP system could prevent some connectivity to systems that support only LM authentication (Windows 95,/98,and Windows for Workgroups) or only NTLM (Windows NT 4.0 prior to Service Pack 4). The Active Directory Services client may be installed on Windows 9x machines to allow for NTLMv2 security. HKLM\System\CurrentControlSet\Control\Lsa\LMCompatibilityLevel = 5 (NSA)	Not Defined	Not Defined	Send NTLMv2 response only\refuse LM and NTLM

Security Options	Multiuser Stand Alone (MUSA)	P2P LAN	client/Server AD
Network security: LDAP client signing requirements **Security Objective:** This policy setting determines the level of data signing that is requested on behalf of clients that issue LDAP BIND requests, as follows: • **None**. The LDAP BIND request is issued with the caller-specified options. • **Negotiate signing**. If Transport Layer Security/Secure Sockets Layer (TLS/SSL) has not been started, the LDAP BIND request is initiated with the LDAP data signing option set in addition to the caller-specified options. If TLS/SSL has been started, the LDAP BIND request is initiated with the caller-specified options. • **Require signature**. This level is the same as **Negotiate signing**. However, if the LDAP server's intermediate saslBindInProgress response does not indicate that LDAP traffic signing is required, the caller is told that the LDAP BIND command request failed. The possible values for the **Network security: LDAP client signing requirements** setting are: • None • Negotiate signing • Require signature • Not Defined ***Vulnerability*** Unsigned network traffic is susceptible to man-in-the-middle attacks in which an intruder captures the packets between the client and server, modifies them, and then forwards them to the server. For an LDAP server, this susceptibility means that an attacker could cause a server to make decisions that are based on false or altered data from the LDAP queries. To lower this risk in your network, you can implement strong physical security measures to protect the network infrastructure. Also, you can make all types of man-in-the-middle attacks extremely difficult if you require digital signatures on all network packets by means of IPsec authentication headers. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies c. Double click on the **Security Options policy** object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. d. Select Local Security Setting Tab of **Network security: LDAP client signing requirements** policy to set options. *Note:* This policy setting does not have any impact on ldap_simple_bind or ldap_simple_bind_s. No Microsoft LDAP clients that are included with Windows XP Professional use ldap_simple_bind or ldap_simple_bind_s to communicate with a domain controller. HKLM\System\CurrentControlSet\Services\LDAP\LDAPClientIntegrity=1	Negotiating Signing	Negotiating Signing	Require Signing

Security Options	Multiuser Stand Alone (MUSA)	P2P LAN	client/Server AD
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients ***Security Objectives:*** This policy setting allows a client computer to require the negotiation of message confidentiality (encryption), message integrity, 128-bit encryption, or NTLMv2 session security. These values are dependent on the **LAN Manager Authentication Level** policy setting value. The possible values for the **Network security: Minimum session security for NTLM SSP based (including secure RPC) clients** setting are: • **Require message confidentiality**. The connection will fail if encryption is not negotiated. Encryption converts data into a form that is not readable until decrypted. • **Require message integrity**. The connection will fail if message integrity is not negotiated. The integrity of a message can be assessed through message signing. Message signing proves that the message has not been tampered with; it attaches a cryptographic signature that identifies the sender and is a numeric representation of the contents of the message. • **Require 128-bit encryption**. The connection will fail if strong encryption (128-bit) is not negotiated. • **Require NTLMv2 session security**. The connection will fail if the NTLMv2 protocol is not negotiated. • **Not Defined**. ***Vulnerability:*** You can enable all of the options for this policy setting to help protect network traffic that uses the NTLM Security Support Provider (NTLM SSP) from being exposed or tampered with by an attacker who has gained access to the same network. In other words, these options help protect against man-in-the-middle attacks. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies a. Double click on the **Security Options policy** object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. b. Select Local Security Setting Tab of **Network security: LDAP client signing requirements** policy to set options. ***Note:*** HKLM\System\CurrentControlSet\Control\Lsa\MSV1_0\NTLMMinClientSec=537395200 (NSA)	Required all four options	Required all four options	Required all four options

Security Options	Multiuser Stand Alone (MUSA)	P2P LAN	client/Server AD
Network security: Minimum session security for NTLM SSP based (including secure RPC) servers ***Security Objective:*** This policy setting allows a server to require the negotiation of message confidentiality (encryption), message integrity, 128-bit encryption, or NTLMv2 session security. These values are dependent on the **LAN Manager Authentication Level** security setting value. The possible values for the **Network security: Minimum session security for NTLM SSP based (including secure RPC) servers** setting are: **Require message confidentiality**. The connection will fail if encryption is not negotiated. Encryption converts data into a form that is not readable by anyone until decrypted. **Require message integrity**. The connection will fail if message integrity is not negotiated. The integrity of a message can be assessed through message signing. Message signing proves that the message has not been tampered with; it attaches a cryptographic signature that identifies the sender and is a numeric representation of the contents of the message. **Require 128-bit encryption**. The connection will fail if strong encryption (128-bit) is not negotiated. **Require NTLMv2 session security**. The connection will fail if the NTLMv2 protocol is not negotiated. **Not Defined**. ***Vulnerability:*** You can enable all of the options for this policy setting to help protect network traffic that uses the NTLM Security Support Provider (NTLM SSP) from being exposed or tampered with by an attacker who has gained access to the same network. That is, these options help protect against man-in-the-middle attacks. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies Double click on the **Security Options policy** object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. Select Local Security Setting Tab of **Network security: Minimum session security for NTLM SSP based (including secure RPC) servers** policy to set options. ***Note:*** HKLM\System\CurrentControlSet\Control\Lsa\MSV1_0\NTLMMinServerSec=537395200 (NSA)	Required all four options	Required all four options	Required all four options

Security Options	Multiuser Stand Alone (MUSA)	P2P LAN	client/Server AD
Recovery console: Allow automatic administrative logon ***Security Objective:*** This policy setting determines whether the Administrator account password must be provided before access to the computer is granted. If you enable this setting, the Administrator account is automatically logged on to the computer at the Recovery Console; no password is required. The possible values for the **Recovery console: Allow automatic administrative logon** setting are: • Enabled • Disabled • Not Defined ***Vulnerability*** The Recovery Console can be very useful when you need to troubleshoot and repair computers that do not start. However, it is dangerous to allow automatic log on to the console. Anyone could walk up to the server, disconnect the power to shut it down, restart it, select **Recover Console** from the **Restart** menu, and then assume full control of the server. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies Double click on the **Security Options policy** object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. Select Local Security Setting Tab of **Recovery console: Allow automatic administrative logon policy** to set options. ***Note:*** HKLM\Software\Microsoft\Windows NT\CurrentVersion\Setup\RecoveryConsole\SecurityLevel=0	Disabled	Disabled	Disabled

Security Options	Multiuser Stand Alone (MUSA)	P2P LAN	client/Server AD
Recovery console: Allow floppy copy and access to all drives and all folders ***Security objective:*** You can enable this policy setting to make the Recovery Console SET command available, which allows you to set the following Recovery Console environment variables. AllowWildCards. Enables wildcard support for some commands (such as the DEL command). AllowAllPaths. Allows access to all files and folders on the computer. AllowRemovableMedia. Allows files to be copied to removable media, such as a floppy disk. NoCopyPrompt. Suppresses the prompt that typically displays before an existing file is overwritten. The possible values for the Recovery console: Allow floppy copy and access to all drives and all folders setting are: Enabled Disabled Not Defined ***Vulnerability:*** An attacker who can cause the system to reboot into the Recovery Console could steal sensitive data and leave no audit or access trail. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies Double click on the Security Options policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. Select Local Security Setting Tab of Recovery console: Allow floppy copy and access to all drives and all folders policy to set options. ***Note:*** HKLM\Software\Microsoft\Windows NT\CurrentVersion\Setup\RecoveryConsole\SetCommand=0	Disabled	Disabled	Disabled

Security Options	Multiuser Stand Alone (MUSA)	P2P LAN	client/Server AD
Shutdown: Allow system to be shut down without having to log on ***Security Objective:*** This policy setting determines whether a computer can be shut down without having to log on to Windows. If you enable this policy setting, the **Shut Down** command is available on the Windows logon screen. If you disable this policy setting, the **Shut Down** option is removed from the Windows logon screen. This configuration requires users to be able to log on to the computer successfully and have the **Shut down the system** user right before they can perform a computer shutdown. The possible values for the **Shutdown: Allow system to be shut down without having to log on** setting are: • Enabled • Disabled • Not Defined ***Vulnerability:*** Users who can access the console locally could shut down the computer. Attackers could also walk to the local console and restart the server, which would cause a temporary DoS condition. Attackers could also shut down the server and leave all of its applications and services unavailable. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies Double click on the **Security Options policy** object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. Select Local Security Setting Tab of **Shutdown: Allow system to be shut down without having to log policy** to set options. ***Note:*** HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\ShutdownWithoutLogon=0	Disabled	Disabled	Disabled

Security Options	Multiuser Stand Alone (MUSA)	P2P LAN	client/Server AD
Shutdown: Clear virtual memory page file ***Security Objective:*** This policy setting determines whether the virtual memory page file is cleared when the computer is shut down. Virtual memory support uses a system page file to swap pages of memory to disk when they are not used. On a running computer, this page file is opened exclusively by the operating system, and it is well protected. However, computers that are configured to allow other operating systems to start might have to make sure that the system page file is wiped clean when the computer shuts down. This confirmation ensures that sensitive information from process memory that might be placed in the page file is not available to an unauthorized user who manages to directly access the page file after shutdown. When you enable this policy setting, the system page file is cleared upon clean shutdown. Also, this policy setting will force the computer to clear the hibernation file Hiberfil.sys when hibernation is disabled on a portable computer. The possible values for the Shutdown: Clear virtual memory page file setting are: • Enabled • Disabled • Not Defined **Vulnerability** Important information that is kept in real memory may be written periodically to the page file to help Windows Server 2003 handle multitasking functions. An attacker who has physical access to a server that has been shut down could view the contents of the paging file. The attacker could move the system volume into a different computer and then analyze the contents of the paging file. Although this process is time consuming, it could expose data that is cached from random access memory (RAM) to the paging file. Caution: An attacker who has physical access to the server could bypass this countermeasure by simply unplugging the server from its power source. Procedure: Under Local Security Policy or Default Domain Security Policy Local Policies Double click on the Security Options policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. Select Local Security Setting Tab of Shutdown: Clear virtual memory page file policy to set options. ***Note:*** HKLM\System\CurrentControlSet\Control\Session Manager\Memory Management\ClearPageFileAtShutdown=1 (NSA)	Enabled	Enabled	Enabled

Security Options	Multiuser Stand Alone (MUSA)	P2P LAN	client/Server AD
System cryptography: Force strong key protection for user keys stored on the computer ***Security Objective:*** This policy setting determines whether users can use private keys, such as their S/MIME key, without a password. The possible values for the **System cryptography: Force strong key protection for user keys stored on the computer** setting are: User input is not required when new keys are stored and used User is prompted when the key is first used User must enter a password each time they use a key Not Defined ***Vulnerability:*** You can configure this policy setting so that users must provide a password that is distinct from their domain password every time they use a key. This configuration makes it more difficult for an attacker to access locally stored user keys, even if the attacker takes control of the user's computer and determines their logon password. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies Double click on the **Security Options policy** object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. Select Local Security Setting Tab of **System cryptography: Force strong key protection for user keys stored on the computer** policy to set options.	Enabled	Enabled	Enabled

Security Options	Multiuser Stand Alone (MUSA)	P2P LAN	client/Server AD
System objects: Default owner for objects created by members of the Administrators group ***Security Objective:*** This policy setting determines whether the **Administrators** group or an object creator is the default owner of any system objects that are created. The possible values for the **System objects: Default owner for objects created by members of the Administrators group** setting are: Administrators group Object creator Not Defined ***Vulnerability*** If you configure this policy setting to **Administrators group**, it will be impossible to hold individuals accountable for the creation of new system objects. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies Double click on the **Security Options policy** object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. Select Local Security Setting Tab of **System objects: Default owner for objects created by members of the Administrators group** policy to set options. ***Note:*** Setting this value to Enabled may result in an inability to connect to HTTPS sites using SSL depending on the encryption algorithm enabled at the site. Problems may also occur when connecting to the Windows Update website. HKLM\System\CurrentControlSet\Control\Lsa\NoDefaultAdminOwner=1	Object Creator	Object Creator	Object Creator

Security Options	Multiuser Stand Alone (MUSA)	P2P LAN	client/Server AD
System objects: Require case insensitivity for non-Windows subsystems ***Security Objective:*** This policy setting determines whether case insensitivity is enforced for all subsystems. The Microsoft Win32® subsystem is case-insensitive. However, the kernel supports case sensitivity for other subsystems, such as Portable Operating System Interface for UNIX (POSIX). If you enable this setting, case insensitivity is enforced for all directory objects, symbolic links, and IO as well as file objects. If you disable this setting, the Win32 subsystem does not become case-sensitive. The possible values for the **System objects: Require case insensitivity for non-Windows subsystems** setting are: Enabled Disabled Not Defined ***Vulnerability:*** Because Windows is case-insensitive but the POSIX subsystem will support case sensitivity, failure to enable this policy setting would make it possible for a user of that subsystem to create a file with the same name as another file but with a different mix of upper and lower case letters. Such a situation could potentially confuse users when they try to access such files from normal Win32 tools because only one of the files will be available. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies Double click on the **Security Options policy** object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. Select Local Security Setting Tab of **System objects: Require case insensitivity for non-Windows subsystems** policy to set options. HKLM\System\CurrentControlSet\Control\Session Manager\Kernel\ ObCaseInsensitive=1	Enabled	Enabled	Enabled

Security Options	Multiuser Stand Alone (MUSA)	P2P LAN	client/Server AD
System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links) ***Security Objective:*** This policy setting determines the strength of the default DACL for objects. Windows maintains a global list of shared computer resources (such as MS-DOS device names, mutexes, and semaphores) so that objects can be located and shared among processes. The possible values for the **System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)** setting are: Enabled Disabled Not Defined ***Vulnerability*** This setting determines the strength of the default DACL for objects. Windows Server 2003 maintains a global list of shared computer resources so that objects can be located and shared among processes. Each type of object is created with a default DACL that specifies who can access the objects and with what permissions. If you enable this setting, the default DACL is strengthened because non-administrator users are allowed to read shared objects but not modify shared objects that they did not create. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies Double click on the **Security Options policy** object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. Select Local Security Setting Tab of **System cryptography: Force strong key protection for user keys stored on the computer** policy to set options. ***Note:*** HKLM\System\CurrentControlSet\Control\Session Manager\ ProtectionMode = 1	Enabled	Enabled	Enabled

Security Options	Multiuser Stand Alone (MUSA)	P2P LAN	client/Server AD
System settings: Optional subsystems ***Security Objective:*** This policy setting determines which subsystems support your applications. You can use this security setting to specify as many subsystems as your environment demands. The possible values for the **System settings: Optional subsystems** setting are: A user-defined list of subsystems Not Defined ***Vulnerability*** The POSIX subsystem is an Institute of Electrical and Electronic Engineers (IEEE) standard that defines a set of operating system services. The POSIX subsystem is required if the server supports applications that use that subsystem. The POSIX subsystem introduces a security risk that relates to processes that can potentially persist across logons. If a user starts a process and then logs out, there is a potential that the next user who logs on to the computer could access the previous user's process. This potential is dangerous, because anything the second user does with that process will be performed with the privileges of the first user. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies Double click on the **Security Options policy** object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. Select Local Security Setting Tab of **System cryptography: Force strong key protection for user keys stored on the computer** policy to set options.	Set to Null Value	Set to Null Value	Set to Null Value

Security Options	Multiuser Stand Alone (MUSA)	P2P LAN	client/Server AD
System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies ***Security Objective:*** This policy setting determines whether digital certificates are processed when software restriction policies are enabled and a user or process attempts to run software with an .exe file name extension. This security setting enables or disables certificate rules (a type of software restriction policies rule). With software restriction policies, you can create a certificate rule that will allow or disallow Authenticode®-signed software to run, based on the digital certificate that is associated with the software. For certificate rules to work in software restriction policies, you must enable this security setting. The possible values for the **System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies** setting are: Enabled Disabled Not Defined ***Vulnerability*** Software restriction policies help to protect users and computers because they can prevent the execution of unauthorized code, such as viruses and Trojans horses. ***Procedure:*** Under Local Security Policy or Default Domain Security Policy Local Policies Double click on the **Security Options policy** object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. Select Local Security Setting Tab of **System cryptography: Force strong key protection for user keys stored on the computer** policy to set options.	Enabled	Enabled	Enabled
Note: In the Windows XP, it is possible to add custom registry settings to the Security Configuration Tool Set. To accomplish this, perform the following actions: Copy the file %SystemRoot%\inf\sceregvl.inf to another file with a different name. This will ensure that a copy of the original exists in case of a problem. Open %SystemRoot%\inf\sceregvl.inf in Notepad, Wordpad, or another text editor Add a line in the form *regpath, type, displayname, displaytype* where *regpath* – registry key value path, e.g.,MACHINE\System\CurrentControlSet\Control\Lsa\AuditBaseObjects *type* – data type of the registry entry represented by a number. Possible values are REG_SZ (1), REG_EXPAND_SZ (2), REG_BINARY (3), REG_DWORD (4), REG_MULTISZ (7) *displayname* – the name actually displayed in the security template, e.g., "Audit the access of global system objects" *displaytype* – How the interface will display the registry value type. Possible values are Boolean (0), number (1), string (2), choices (3), multivalued (4), bitmask (5). Values 4 and 5 are available on Windows XP only. If choices are specified, the choices should then be specified in the format *value1|display1,value2|display2,…* Re-register scecli.dll by executing regsvr32 scecli.dll at a command prompt			

More Information

The following links provide additional information about security options in Windows Server 2003 and Windows XP.

- For more information about default COM machine access restrictions in Windows XP, see the "Managing Windows XP Service Pack 2 Features Using Group Policy: Security-Related Policy Settings" guide at www.microsoft.com/technet/prodtechnol/winxppro/maintain/mangxpsp2/mngsecps.mspx.
- For information about default COM access restrictions in Windows Server 2003 with SP1, see the "DCOM Security Enhancements" section in the "Changes to Functionality in Microsoft Windows Server 2003 Service Pack 1" guide at www.microsoft.com/technet/prodtechnol/windowsserver2003/library/BookofSP1/.
- For more information about how to enable NTLMv2, see the Microsoft Knowledge Base article "How to enable NTLM 2 authentication" at http://support.microsoft.com/default.aspx?scid=239869.
- For more information about how to ensure that more secure LAN Manager Authentication Level settings work in networks with a mix of Windows 2000 and Windows NT® 4.0 computers, see the Microsoft Knowledge Base article "Authentication Problems in Windows 2000 with NTLM 2 Levels Above 2 in a Windows NT 4.0 Domain" at http://support.microsoft.com/?scid=305379.
- For more information about LAN Manager compatibility levels, see the Microsoft Knowledge Base article "Client, service, and program incompatibilities that may occur when you modify security settings and user rights assignments" at http://support.microsoft.com/?scid=823659.
- For more information about NTLMv2 authentication, see the Microsoft Knowledge Base article "How to Enable NTLM 2 Authentication" at http://support.microsoft.com/?scid=239869.
- For more information about how to restore default security settings locally, see Microsoft Knowledge Base article "How to Reset Security Settings Back to the Defaults" at http://support.microsoft.com/?scid=313222.
- For more information about how to restore default security settings in the built-in domain Group Policy objects, see Microsoft Knowledge Base Article "How to Reset User Rights in the Default Domain Group Policy in Windows Server 2003" at http://support.microsoft.com/?scid=324800.

5. Event Log

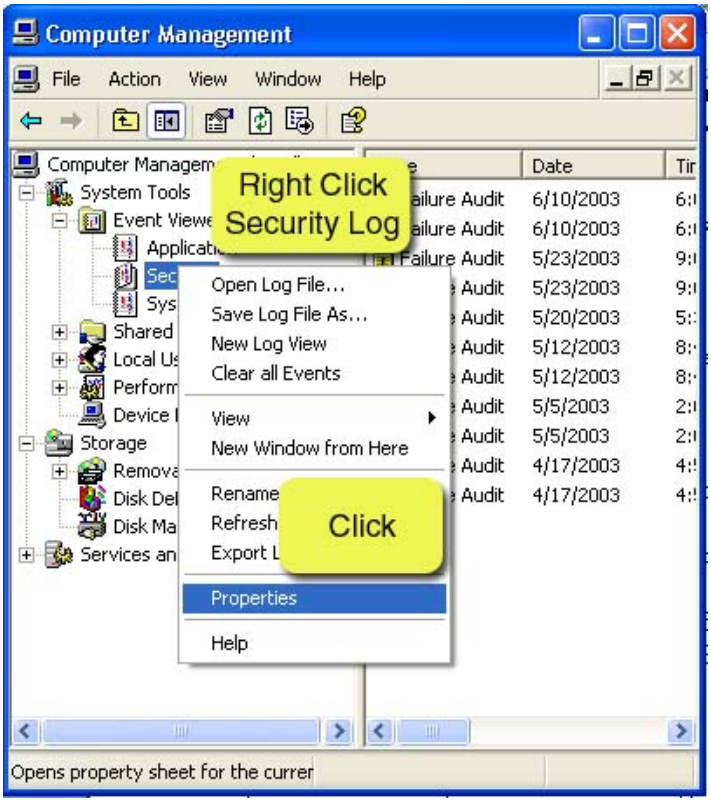
The event log records events on the computer, and the Security log records audit events. The event log container of Group Policy is used to define the attributes that are related to the Application, Security, and System event logs, such as maximum log size, access rights for each log, and retention settings and methods. You can configure the event log settings in the following location within the Group Policy Object Editor:

Computer Configuration\Windows Settings\Security Settings
Event Log\Settings for Event Logs

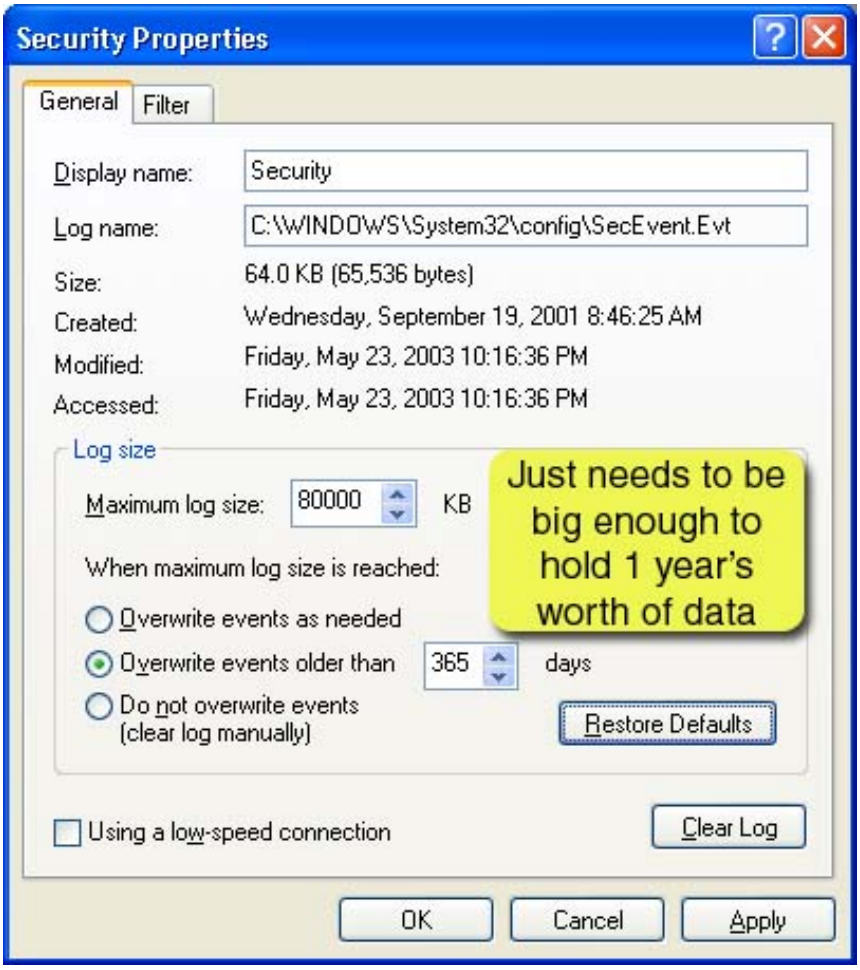
Or Manually configure it via the following procedure:

- Click Start
2 - Right-Click "My Computer"
3 - Click "Manage"

4 - Click the "+" next to Event Viewer.



5 - Right-click Security Log
6 - Click properties.



7 - In the example, the Maximum log size is set at 80,000 KB. Even though we are backing up the file periodically we will use this setting uniformly as a protective measure.

Click OK when finished.

Event Logs Policies	Multiuser Stand Alone (MUSA)	P2P LAN	Client/Server AD
Maximum event log size **Security Objective:** This policy setting specifies the maximum size of the Application, Security, and System event logs. Although the user interfaces (UIs) of both the Group Policy Object Editor and the Microsoft Management Console (MMC) Event Viewer snap-in allow you to enter values as large as four GB, certain factors make the effective maximum size for these logs much smaller. The **Event Log** service uses memory-mapped files, and it runs as one of the services under the Services.exe process as Eventlog.dll. When files are loaded in this way, the entire file is loaded into the computer's memory. All of the current versions of Microsoft Windows® have an architectural limitation with regard to memory-mapped files: no process can have more than one GB of memory-mapped files in total. This limitation means that all of the services that run under the Services.exe process must share the one GB pool. The memory is assigned in contiguous 64 KB portions, and if the computer cannot assign additional memory to expand memory-mapped files, problems will occur. For the **Event Log** service, the use of memory-mapped files means that regardless of the amount of memory that the **Maximum event log size** setting specifies, log events may no longer be recorded in the log when the computer has no more memory available for the memory-mapped file. Error messages will not be displayed; the events will simply not appear in the event log, or they may overwrite other events that had been recorded previously. Fragmentation of the log files within memory has also been shown to lead to significant performance problems on busy computers. Because of these limitations—even though the theoretical limit for memory-mapped files suggests otherwise and the Event Viewer and Group Policy Object Editor UIs allow you to specify as much as four GB per log—Microsoft has verified that the practical limit is approximately 300 MB on most servers-- that is, 300 MB for *all of the event logs combined*. On Microsoft Windows XP, member servers, and stand-alone servers, the combined size of the Application, Security, and System event logs should not exceed 300 MB. On domain controllers, the combined size of these three logs plus the Active Directory® directory service, DNS, and Replication logs should not exceed 300 MB. These limitations have caused problems for some Microsoft customers, but the only way to remove the limitations requires fundamental changes to the way system events are recorded. Microsoft is rewriting the event log system to resolve these problems in the next version of Windows.	Security Log =80MB, System Log =80MB,Application Log=80MB	Security Log =80MB, System Log =80MB,Application Log=80MB	Security Log =80MB, System Log =80MB,Application Log=80MB

Event Logs Policies	Multiuser Stand Alone (MUSA)	P2P LAN	Client/Server AD
Maximum event log size (continued) If you significantly increase the number of objects to audit in your organization, there is a risk that the Security log will reach its capacity and force the computer to shut down if you enabled the **Audit: Shut down system immediately if unable to log security audits** setting. If such a shutdown occurs, the computer will be unusable until an administrator clears the Security log. To prevent such a shutdown, you can disable the **Audit: Shut down system immediately if unable to log security audits** setting that is described in above section of "Security Options," and increase the Security log size. Alternatively, you can configure automatic log rotation as described in the Microsoft Knowledge Base article "The event log stops logging events before reaching the maximum log size" at http://support.microsoft.com/default.aspx?kbid=312571. **Procedure:** **Event Log → Settings for Event Logs** → specific option to view or edit (see detail steps above)			
Prevent local guests group from accessing event logs ***Security Objective:*** This policy setting determines whether guests can access the Application, Security, and System event logs. The possible values for the **Prevent local guests group from accessing event logs** setting are: Enabled Disabled Not Defined ***Note:*** This policy setting does not appear in the Local Computer Policy object. This policy setting only affects computers that run Windows 2000 and subsequent versions of Windows. Vulnerability An attacker who has successfully logged onto a computer with guest privileges could learn important information about the computer if they were able to view the event logs. The attacker could then use this information to implement additional exploits. **Procedure:** **Event Log → Settings for Event Logs** → specific option to view or edit (see detail steps above) Enable the **Prevent local guests group from accessing event logs** setting for the policies of all three event logs.	Enabled	Enabled	Enabled

Event Logs Policies	Multiuser Stand Alone (MUSA)	P2P LAN	Client/Server AD
Retain event logs **Security Objective:** This policy setting determines the number of days of event log data to retain for the Application, Security, and System logs if the retention method that is specified for the log is **By Days**. Configure this setting only if you archive the log at scheduled intervals and you make sure that the maximum log size is large enough to accommodate the interval. The possible values for the **Retain event logs** setting are: A user-defined number in days between 1 and 365 Not Defined **Note**: This policy setting does not appear in the Local Computer Policy object. A user must be assigned the **Manage auditing and security log** user right to access the Security log. Vulnerability If you archive the log at scheduled intervals: Open the **Properties** dialog box for this policy. Specify the appropriate number of days in the **Retain application log** setting. Select **Overwrite events by days** for the event log retention method. Also, ensure that the maximum log size is large enough to accommodate the interval.	Enabled	Enabled	Enabled

Event Logs Policies	Multiuser Stand Alone (MUSA)	P2P LAN	Client/Server AD
Retention method for event log **Security Objective:** This policy setting determines the wrapping method for the Application, Security, and System logs. If you do not want to archive the Application log: Open the **Properties** dialog box for this policy. Select the **Define this policy setting** check box. Click **Overwrite events as needed**. If you want to archive the log at scheduled intervals: Open the **Properties** dialog box for this policy. Select the **Define this policy setting** check box. Click **Overwrite events by days.** Specify the appropriate number of days in the **Retain application log** setting. Ensure that the maximum log size is large enough to accommodate the interval. If you must retain all the events in the log: Open the **Properties** dialog box for this policy. Select the **Define this policy setting** check box. Click **Do not overwrite events (clear log manually)**. This option requires that the log be cleared manually. In this configuration, new events are discarded when the maximum log size is reached. The possible values for the **Retention method for event log** setting are: Overwrite events by days Overwrite events as needed Do not overwrite events (clear log manually) Not defined **Note**: This policy setting does not appear in the Local Computer Policy object. Vulnerability If you significantly increase the number of objects to audit in your organization, there is a risk that the Security log will reach its capacity and force the computer to shut down. If such a shutdown occurs, the computer will be unusable until an administrator clears the Security log. To prevent such a shutdown, you can disable the **Audit: Shut down system immediately if unable to log security audits** setting that is described in Chapter 5, "Security Options" and then increase the Security log size. If you set the **Event log retention method** to **Manual** or **Overwrite events by days**, it is possible for important recent events to not be recorded or for a DoS attack to occur.	365 Days	365 Days	365 Days

Event Logs Policies	Multiuser Stand Alone (MUSA)	P2P LAN	Client/Server AD
Delegating Access to the Event Logs In Microsoft Windows Server™ 2003, it is possible to customize the permissions on each event log on a computer. This capability was not available in previous versions of Windows. Some organizations may want to grant read-only access to one or more of the System event logs to some members of the IT team. The access control list (ACL) is stored as a Security Descriptor Definition Language (SDDL) string, in a REG_SZ value called "CustomSD" for each event log in the registry, as in the following example: **HKEY_LOCAL_MACHINE\System\CurrentControlSet\ Services\EventLog\CustomSDCreate a REG_SZ registry value O:BAG:SYD:(D;;0xf0007;;;AN)(D;;0xf0007;;;BG) (A;;0xf0007;;;SY)(A;;0x7;;;BA)(A;;0x5;;;SO)(A;;0x1;;;IU)(A;;0x1;;;SU) (A;;0x1;;;S-1-5-3)(A;;0x2;;;LS)(A;;0x2;;;NS)** If you edit this value and restart the computer, the new setting will take effect. **Caution**: Be careful when you edit the registry values, because there is no "undo" function in the Registry Editor tool. If you make a mistake, you will have to correct it manually. Also, you could accidentally configure the ACLs on an event log in such a way that no one could access it. Be certain that you fully understand SDDL and the default permissions that are placed on each event log before you proceed. Also, be certain to test any changes thoroughly before you implement them in a production environment. For more information about how to configure security for event logs in Windows Server 2003, see "How to: Set Event Log Security Locally or by Using Group Policy in Windows Server 2003" at http://support.microsoft.com/default.aspx?kbid=323076.	Not Enabled	Not Enabled	Not Enabled

Event Logs Policies	Multiuser Stand Alone (MUSA)	P2P LAN	Client/Server AD
Note: **Saving And Clearing the Audit Logs** To save and clear the logs: Select **Start → All Programs → Administrative Tools → Event Viewer** ▪ Click on the log to be cleared in the right pane of the Event Viewer window ▪ Select **Clear All Events** recommended **Action** menu ▪ Click **Yes** to save settings with unique file name ▪ Specify where the log will be saved and then click **Save** ▪ Click **Yes** to clear the log ▪ Repeat the above steps for each log Resetting the Audit Log Settings After the System Halts If the system halts as a result of an audit failure, an administrator must restart the system and use the registry editor (regedit.exe) to modify the following registry key value: Hive: **HKEY_LOCAL_MACHINE** Key: **\System\CurrentControlSet\Control\Lsa** Name: **CrashOnAuditFail** Type: **REG_DWORD** Value: 1 **NOTE: This value is set by the operating system just before it crashes due to an audit log failure. While the value is 2, only the administrator can log on to the computer. This value confirms the cause of the crash. Reset the value**			

More Information

The following links provide additional information about event logging in Windows Server 2003 and Windows XP.

- For more information about how to configure security for event logs in Windows Server 2003, see "How to: Set Event Log Security Locally or by Using Group Policy in Windows Server 2003" at http://support.microsoft.com/default.aspx?kbid=323076.
- For more information about SDDL, see "Security Descriptor Definition Language" on MSDN at http://msdn.microsoft.com/library/default.asp?url=/library/en-us/secauthz/security/security_descriptor_definition_language.asp.

6. Restricted Groups

The Restricted Groups option allows the administrator to manage the membership of sensitive groups. For example, if the Administrators group is to only consist of the built-in Administrator account, the Administrators group can be added to the Restricted Groups option and Administrator can be added in the **Members of Administrators** column. This setting could prevent other users from elevating their privilege to the Administrators group through various attack tools and hacks.

Not all groups need to be added to the Restricted Group list. It is recommended that only sensitive groups be configured through security templates. Any groups not listed will retain their membership lists.

NIST recommends that all users be removed from the Remote Desktop Users group on all systems in all environments, except for those users that specifically need to belong to the group. This will reduce the possibility of someone gaining unauthorized access to the system through Remote Desktop. NIST also recommends restricting membership in the Power Users group because it is nearly equivalent in privileges to the Administrators group. Users should not use an account in the Power Users group to operate a system on a daily basis; such accounts should be treated as Administrators group accounts and used only when necessary. Whenever possible, users who need additional privileges, but not full administrative level access, should be granted the individual privileges needed instead of the range of privileges granted by Power Users group membership. By default, each NIST security template removes all users from the Remote Desktop Users and Power Users groups; the Specialized Security-Limited Functionality template also removes all users from the Backup Operators group. (NIST)

The Restricted Groups option allows the administrator to manage the membership of sensitive groups. This setting could prevent other users from elevating their privilege to the Administrators group through various attack tools and hacks.

Not all groups need to be added to the Restricted Group list. It is recommended that only sensitive groups be configured through security templates. Any groups not listed will retain their membership lists.

The recommended setting in the provided workstation template restricts the Power Users group to having no members. This is generally good security practice. However, environments using older applications or custom written line-of-business applications may require users to have additional privileges similar to the Power Users group on certain files, folders, or registry keys relating to those applications. Ideally, the needed permissions on these files and registry keys should be identified and implemented instead of adding users to the Power Users group. Under no circumstances should you add users to the Administrators group just to make your applications work. (NSA/DISA)

Restricted Group	Multiuser Stand Alone	P2P LAN	Client/Server AD
Backup Operators ***Power Users*** ***Remote Desktop Users***	None	None	None

7. File System Security

7.1 NTFS

NTFS file system is vastly superior to the other XP file system options—FAT16 and FAT32. Neither FAT16 nor FAT32 provides features for establishing access control for files or encrypting files. The recommendation is to convert to NTFS or use NTFS from the start. Conversion can be achieved with the use of convert.exe.

You can also configure the file system security settings at the following location in the Group Policy Object Editor:

Computer Configuration\Windows Settings\Security Settings\File System

7.1.1 Alternative Data Stream (specific for NTFS)

Alternative Data Stream support was added to NTFS (Windows NT, Windows 2000 and Windows XP) to help support Macintosh Hierarchical File System (HFS) which uses stores other information for a file. While this is the intended use (as well as a few Windows internal functions) there or other uses for Alternative Data Streams that should concern security professionals. Using Alternative Data Streams a user can easily hide files that can go undetected unless closely inspection.

Some anti-malware tools understand how to search Alternate Data Streams for malware and they can recognize known spyware in Alternative Data Stream. Other tools are also available to scan the storage devices for hidden files. Most noticeable change would be the changes in the disk storage free space when hidden files have been added. Although the number of files remained constant when listed, the free space would have shown decreased as an indication that hidden files have been introduced.

7.2 Folder Options

Modifying the Folder Options can greatly improve defenses against malware. The system can be configured to show all filenames fully, including their extensions. In addition, Folder Options contains the associations between file types and the default applications that run each file type. By modifying the associations for file extensions that are often used for malicious purposes, such files will be run by the Notepad application, which effectively neutralizes them.

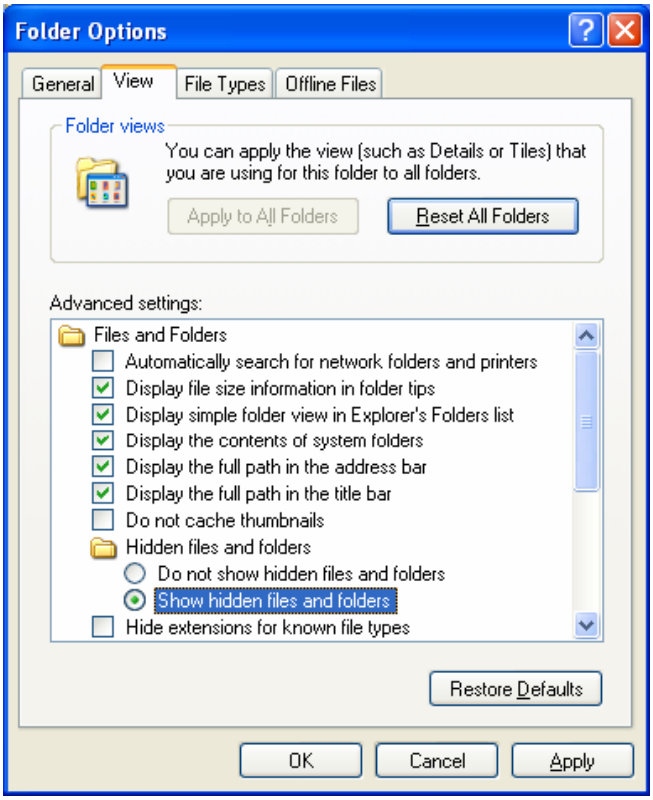
The recommendation is to set Folder options to display all hidden files and extensions. Exclusively, disable the simple file sharing options so that security tab may be accessed.

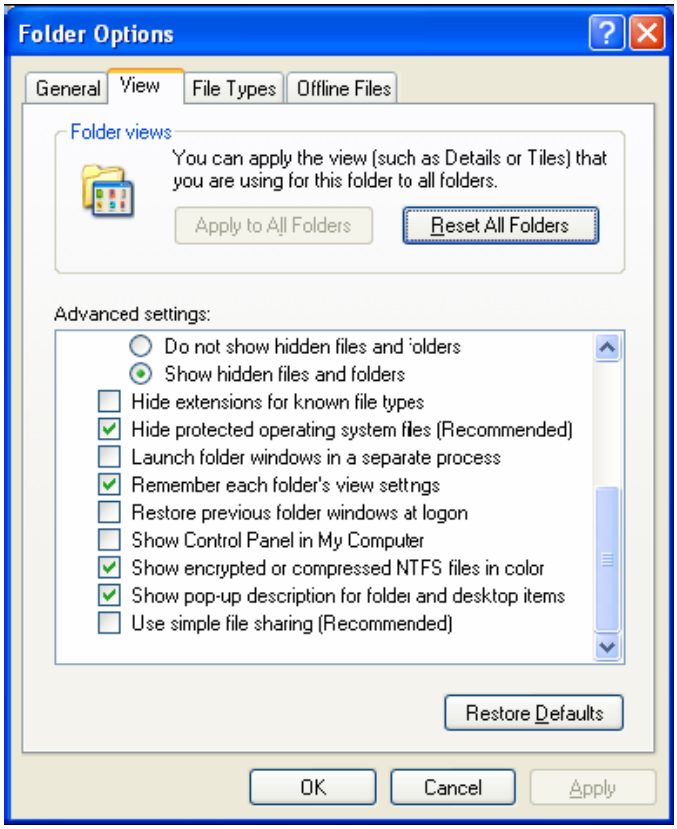
You can perform the following steps to modify the Folder Options:

1. Click the **Start** menu and choose **Control Panel**.
2. Select **Folder Options**.
3. Verify that the **Show common tasks in folders**, **Open each folder in the same window**, and
4. **Double-click to open an item (single-click to select)** radio buttons are selected.
5. Select the **View** tab. Adjust the settings so that they match the check boxes and radio buttons
6. Select the **File Types** tab. Scroll down the registered file types window to select the **JS** extension
7. and click the **Change** button.

8. Select the **Notepad** program and click **OK**.
9. Repeat the previous two steps to change the mapping for the following extensions: **JSE**, **OTF**,**REG**, **SCT**, **SHB**, **SHS, VBE, VBS**, **WSC**, **WSF**, and **WSH**.
10. Click the **Close** button and click **OK**.

See Figures below.





7.3 FILE Permission

These are file permissions for files that can typically be found on Windows XP systems. Note that not all of these resources are available on all Windows XP versions and installations. The same file permissions are used for all NIST templates. Additional files are NISPOM files (or security relevant objects)

The NIST security templates restrict access to 32 executables, protecting them from unauthorized modification and usage. Additional custom settings may be added that are specific to the environment in which the Windows XP machine resides. Please note NIST does not offer any additional integrity check such as auditing of these files. However, it is implicit that a Fail access to these objects would be recorded in the security event log. (NIST)

By Defaults, Microsoft security setting provided the file permission for operation systems file security. NISPOM setting of 142 objects are listed below.

Additionally, NISPOM chapter 8 requires file permission to be set for anti-virus software under the program files folders. For some vendors, antivirus installation also involved common shared files. For example c:\Program Files\ Common Files\Symantec Shared. Permissions for these files should be Administrators, System, with full control and users have read and execute permissions.
Beside anti-virus installed under program file directory, the back up security log folder should only be accessible by administrators or the auditors.

File Permission		Multiuser Stand alone (MUSA) P2P LAN Client/Server AD
%SystemRoot%\system32\arp.exe %SystemRoot%\system32\at.exe %SystemRoot%\system32\attrib.exe %SystemRoot%\system32\cacls.exe %SystemRoot%\system32\debug.exe %SystemRoot%\system32\edlin.exe %SystemRoot%\system32\eventcreate.exe %SystemRoot%\system32\eventtriggers.exe %SystemRoot%\system32\ftp.exe %SystemRoot%\system32\nbtstat.exe %SystemRoot%\system32\net.exe %SystemRoot%\system32\net1.exe %SystemRoot%\system32\netsh.exe %SystemRoot%\system32\netstat.exe %SystemRoot%\system32\nslookup.exe %SystemRoot%\system32\ntbackup.exe	%SystemRoot%\system32\rcp.exe %SystemRoot%\system32\reg.exe %SystemRoot%\system32\regedit.exe %SystemRoot%\system32\regedt32.exe %SystemRoot%\system32\regini.exe %SystemRoot%\system32\regsvr32.exe %SystemRoot%\system32\rexec.exe %SystemRoot%\system32\route.exe %SystemRoot%\system32\rsh.exe %SystemRoot%\system32\sc.exe %SystemRoot%\system32\secedit.exe %SystemRoot%\system32\subst.exe %SystemRoot%\system32\systeminfo.exe %SystemRoot%\system32\ telnet.exe %SystemRoot%\system32\tftp.exe %SystemRoot%\system32\tlntsvr.exe %SystemRoot%\setupapi.log	Administrators, Systems Full control, Users Read & Execute
%SystemRoot%\Temp Folder containing temporary files.	Administrators Full Control, CREATOR OWNER Full Control (Subfolders and files only), SYSTEM Full Control, Users Traverse folder, Create files, Create folders (This folder and sub folders)	Administrators Full Control, CREATOR OWNER Full Control (Subfolders and files only), SYSTEM Full Control, Users Traverse folder, Create files, Create folders (This folder and sub folders)

File Permission		Multiuser Stand alone (MUSA) P2P LAN Client/Server AD
%SystemRoot%\system32\spool\Printers Printer spool.	Administrators Full Control, CREATOR OWNER Full Control (Subfolders and files only), SYSTEM Full Control, Users Traverse folder, Create files, Create folders (This folder and sub folders)	Administrators Full Control, CREATOR OWNER Full Control (Subfolders and files only), SYSTEM Full Control, Users Traverse folder, Create files, Create folders (This folder and sub folders)

File Permission		Multiuser Stand alone (MUSA) P2P LAN Client/Server AD
%SystemRoot%\Registration\CRMLog	Administrators Full Control, CREATOR OWNER Full Control (Subfolders and files only), SYSTEM Full Control (Subfolders and files only), Users Traverse folder, List folder, Read attributes, Read extended attributes, Create files, Read permissions (This folder only) Read data, Read attributes, Read extended attributes, Write data, Append data, Write attributes, Write extended attributes, Delete, Read permissions (Files only)	Administrators Full Control, CREATOR OWNER Full Control (Subfolders and files only), SYSTEM Full Control (Subfolders and files only), Users Traverse folder, List folder, Read attributes, Read extended attributes, Create files, Read permissions (This folder only) Read data, Read attributes, Read extended attributes, Write data, Append data, Write attributes, Write extended attributes, Delete, Read permissions (Files only)

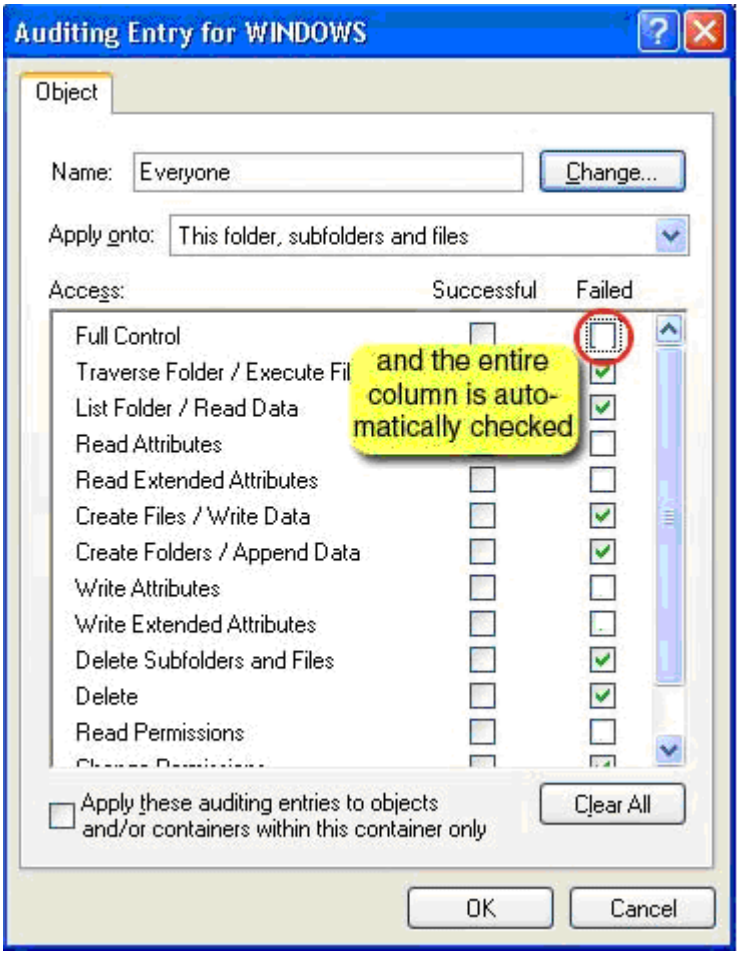
File Permission		Multiuser Stand alone (MUSA) P2P LAN Client/Server AD
%SystemRoot%\system32\activeds.dll %SystemRoot%\system32\adsldpc.dll %SystemRoot%\system32\advapi32.dll %SystemRoot%\system32\advpack.dll %SystemRoot%\system32\apphelp.dll %SystemRoot%\system32\atl.dll %SystemRoot%\system32\authz.dll %SystemRoot%\system32\bootvid.dll %SystemRoot%\system32\browseui.dll %SystemRoot%\system32\cabinet.dll %SystemRoot%\system32\cdfview.dll %SystemRoot%\system32\certcli.dll %SystemRoot%\system32\cfgmgr32.dll %SystemRoot%\system32\clusapi.dll %SystemRoot%\system32\comctl32.dll %SystemRoot%\system32\comdlg32.dll %SystemRoot%\system32\comres.dll %SystemRoot%\system32\credui.dll %SystemRoot%\system32\crypt32.dll %SystemRoot%\system32\cryptdll.dll %SystemRoot%\system32\cryptui.dll %SystemRoot%\system32\cscdll.dll %SystemRoot%\system32\dbghelp.dll %SystemRoot%\system32\devmgr.dll %SystemRoot%\system32\dhcpcsvc.dll %SystemRoot%\system32\dnsapi.dll %SystemRoot%\system32\drivers\ksecdd.sys %SystemRoot%\system32\DRIVERS\ntfs.sys %SystemRoot%\system32\duser.dll %SystemRoot%\system32\efsadu.dll %SystemRoot%\system32\esent.dll %SystemRoot%\system32\eventlog.dll %SystemRoot%\system32\gdi32.dll %SystemRoot%\system32\hal.dll %SystemRoot%\system32\ imagehlp.dll %SystemRoot%\system32\imm32.dll %SystemRoot%\system32\ inetcomm.dll %SystemRoot%\system32\iphlpapi.dll %SystemRoot%\system32\kerberos.dll %SystemRoot%\system32\kernel32.dll %SystemRoot%\system32\linkinfo.dll %SystemRoot%\system32\loadperf.dll %SystemRoot%\system32\lsasrv.dll %SystemRoot%\system32\lsass.exe %SystemRoot%\system32\lz32.dll %SystemRoot%\system32\mfc42u.dll %SystemRoot%\system32\mlang.dll %SystemRoot%\system32\mobsync.dll %SystemRoot%\system32\mpr.dll %SystemRoot%\system32\mprapi.dll %SystemRoot%\system32\mprui.dll	%SystemRoot%\system32\msgina.dll %SystemRoot%\system32\mshtml.dll %SystemRoot%\system32\msi.dll %SystemRoot%\system32\msimg32.dll %SystemRoot%\system32\msoert2.dll %SystemRoot%\system32\msrating.dll %SystemRoot%\system32\mssign32.dll %SystemRoot%\system32\msv1_0.dll %SystemRoot%\system32\msvbvm60.dll %SystemRoot%\system32\msvcp60.dll %SystemRoot%\system32\msvcrt.dll %SystemRoot%\system32\mswsock.dll %SystemRoot%\system32\nddeapi.dll %SystemRoot%\system32\netapi32.dll %SystemRoot%\system32\netcfgx.dll %SystemRoot%\system32\netman.dll %SystemRoot%\system32\netplwiz.dll %SystemRoot%\system32\netrap.dll %SystemRoot%\system32\netshell.dll %SystemRoot%\system32\netui0.dll %SystemRoot%\system32\netui1.dll %SystemRoot%\system32\netui2.dll %SystemRoot%\system32\ntdll.dll %SystemRoot%\system32\ntdsapi.dll %SystemRoot%\system32\ntlanman.dll %SystemRoot%\system32\ntoskrnl.exe %SystemRoot%\system32\odbc32.dll %SystemRoot%\system32\ole32.dll %SystemRoot%\system32\oleacc.dll %SystemRoot%\system32\oleaut32.dll %SystemRoot%\system32\oledlg.dll %SystemRoot%\system32\olepro32.dll %SystemRoot%\system32\pautoenr.dll %SystemRoot%\system32\powrprof.dll %SystemRoot%\system32\printui.dll %SystemRoot%\system32\psapi.dll %SystemRoot%\system32\query.dll %SystemRoot%\system32\rasapi32.dll %SystemRoot%\system32\rasdlg.dll %SystemRoot%\system32\rasman.dll %SystemRoot%\system32\regapi.dll %SystemRoot%\system32\rpcrt4.dll %SystemRoot%\system32\rtutils.dll %SystemRoot%\system32\samlib.dll %SystemRoot%\system32\samsrv.dll %SystemRoot%\system32\sceeli.dll %SystemRoot%\system32\secur32.dll	Administrators, Systems Full Control, Users Read & Execute (NISPOM turns on audit for these objects)

%SystemRoot%\system32\msgina.dll %SystemRoot%\system32\mshtml.dll %SystemRoot%\system32\msi.dll %SystemRoot%\system32\msimg32.dll %SystemRoot%\system32\msoert2.dll %SystemRoot%\system32\msrating.dll %SystemRoot%\system32\mssign32.dll %SystemRoot%\system32\msv1_0.dll %SystemRoot%\system32\msvbvm60.dll %SystemRoot%\system32\msvcp60.dll %SystemRoot%\system32\msvcrt.dll %SystemRoot%\system32\mswsock.dll %SystemRoot%\system32\nddeapi.dll %SystemRoot%\system32\netapi32.dll %SystemRoot%\system32\netcfgx.dll %SystemRoot%\system32\netman.dll %SystemRoot%\system32\netplwiz.dll %SystemRoot%\system32\netrap.dll %SystemRoot%\system32\netshell.dll %SystemRoot%\system32\netui0.dll %SystemRoot%\system32\netui1.dll %SystemRoot%\system32\netui2.dll %SystemRoot%\system32\ntdll.dll %SystemRoot%\system32\ntdsapi.dll %SystemRoot%\system32\ntlanman.dll %SystemRoot%\system32\ntoskrnl.exe %SystemRoot%\system32\odbc32.dll %SystemRoot%\system32\ole32.dll %SystemRoot%\system32\oleacc.dll %SystemRoot%\system32\oleaut32.dll %SystemRoot%\system32\oledlg.dll %SystemRoot%\system32\olepro32.dll %SystemRoot%\system32\pautoenr.dll %SystemRoot%\system32\powrprof.dll %SystemRoot%\system32\printui.dll %SystemRoot%\system32\psapi.dll %SystemRoot%\system32\query.dll %SystemRoot%\system32\rasapi32.dll %SystemRoot%\system32\rasdlg.dll %SystemRoot%\system32\rasman.dll %SystemRoot%\system32\regapi.dll %SystemRoot%\system32\rpcrt4.dll %SystemRoot%\system32\rtutils.dll %SystemRoot%\system32\samlib.dll %SystemRoot%\system32\samsrv.dll %SystemRoot%\system32\scecli.dll %SystemRoot%\system32\secur32.dll setupapi.dll	%SystemRoot%\system32\security.dll %SystemRoot%\system32\setupapi.dll %SystemRoot%\system32\sfc.dll %SystemRoot%\system32\sfcfiles.dll %SystemRoot%\system32\shdocvw.dll %SystemRoot%\system32\shlwapi.dll %SystemRoot%\system32\shsvcs.dll %SystemRoot%\system32\tapi32.dll %SystemRoot%\system32\urlmon.dll %SystemRoot%\system32\user32.dll %SystemRoot%\system32\userenv.dll %SystemRoot%\system32\utildll.dll %SystemRoot%\system32\uxtheme.dll %SystemRoot%\system32\version.dll %SystemRoot%\system32\w32topl.dll %SystemRoot%\system32\wininet.dll %SystemRoot%\system32\winipsec.dll %SystemRoot%\system32\winlogon.exe %SystemRoot%\system32\winmm.dll %SystemRoot%\system32\winscard.dll %SystemRoot%\system32\winspool.drv %SystemRoot%\system32\winsta.dll %SystemRoot%\system32\wintrust.dll %SystemRoot%\system32\wldap32.dll %SystemRoot%\system32\wmi.dll %SystemRoot%\system32\ws2_32.dll %SystemRoot%\system32\ws2help.dll %SystemRoot%\system32\wsock32.dll %SystemRoot%\system32\wtsapi32.dll %SystemRoot%\system32\wzcdlg.dll %SystemRoot%\system32\wzcsapi.dll %SystemRoot%\system32\wzcsvc.dll %SystemRoot%\system32\kdcom.dll %Program File%\Common file\Vendor Antivirus shared % Program File%\Vendor Antivirus directories\antivirus engine % Program File%\Vendor Antivirus directories\antivirus definition	Administrators, Systems Full Control, Users Read & Execute (NISPOM turns on audit for these objects)

7.4 Individual File Auditing

Windows XP provides a method to monitor access to any file stored on an NTFS-formatted partition. This auditing method is typically used to monitor access to sensitive files including security relevant files. To configure individual file auditing, perform the following steps:

1. Right-click on the file, and then select **Properties**.
2. Select the **Security** tab and click on **Advanced**.
3. Select the **Auditing** tab and click on **Add for** specify a user or group.
4. As shown in Figure 7-4, select the file permission access attributes that should be audited by clicking in the appropriate **Successful** and **Failed** check boxes.



8. System Services

System services are described differently than the other settings in this guide because the vulnerability, countermeasure, and potential impact statements are almost identical for all services.

8.1 Service Overview

A service must log on to access resources and objects in the operating system, and most services are not designed to have their default logon account changed

Windows Server 2003 includes three built-in local accounts that are used as the logon accounts for various system services:

Local System account. The Local System account is a powerful account that has full access to the computer and acts as the computer on the network. If a service uses the Local System account to log on to a domain controller, that service has access to the entire domain.

Local Service account. The Local Service account is a special, built-in account that is similar to an authenticated user account. It has the same level of access to resources and objects as members of the **Users** group.

Network Service account. The Network Service account is also a special, built-in account that is similar to an authenticated user account. Like the Local Service account, it has the same level of access to resources and objects as members of the **Users** group, which helps safeguard your computer.

You can configure the system services settings in the following location within the Group Policy Object Editor:

Computer Configuration\Windows Settings\Security Settings
System Services

8.2 Vulnerability

Any service or application is a potential point of attack. Therefore, you should disable or remove any unneeded services or executable files in your environment. There are additional optional services available in Windows Server 2003, such as Certificate Services, that are not installed during a default installation of the operating system.

If compromised, services may offer direct access to system resources or fall victim to buffer overflows or denial of service attacks. Therefore, the proper configuration of services is an important security step. Since services are environment and application specific, no services are configured specifically under NSA/DISA or NISPOM. However, there are a few guidelines to consider when configuring services:

Only run necessary services. For example, if the telnet service or FTP service is running on a system, but not being used, disable it.

Ensure that only a limited number of users/groups can start, stop, or change a service.

If a service is listed, but not needed, change the startup mode to Disabled instead of Manual. This will ensure that the service cannot be restarted by an unauthorized or malicious user. Also, if a service is currently disabled and will remain that way, it is recommended that it be explicitly set to Disabled versus "Not defined."

When configuring either the startup mode or access control list for a service, you must configure the other as well. When a service is explicitly disabled, its ACL should also be secured by changing the default ACL from Everyone Full Control to grant Administrators and SYSTEM Full Control and Authenticated Users Read access.

Run services with the least privilege necessary. For example, do not run a service as a domain administrator if user privileges are sufficient.

8.3 Service Settings

System Services	Setting
Alerter	Disabled
Application Layer Gateway Service	Not Defined
Application Management	Not Defined
Automatic Updates	Disabled
Background Intelligent Transfer Service	Not Defined
ClipBook	Not Defined
COM+ Event System	Not Defined
COM+ System Application	Not Defined
Computer Browser	Not Defined
Cryptographic Services	Not Defined
DHCP Client	Not Defined
Distributed Link Tracking Client	Not Defined
Distributed Transaction Coordinator	Not Defined
DNS Client	Not Defined
Error Reporting Service	Not Defined
Event Log	Not Defined
Fast User Switching Compatibility	Not Defined
Fax	Disabled

FTP Publishing Service	Not Defined
Help and Support	Not Defined
Human Interface Device	Not Defined
Access Not defined	Not Defined
IIS Admin Service	Not Defined
IMAPI CD-Burning	Not Defined
COM Service	Not Defined
Indexing Service	Not Defined
Infrared Monitor	Not Defined
Internet Connection	Not Defined
Firewall (ICF)/Internet	Not Defined
Connection Sharing	Not Defined
(ICS)	Not Defined
IPSEC Services	Not Defined
Logical Disk Manager	Not Defined
Logical Disk Manager Administrative Service	Not Defined
Messenger	Disabled
MS Software Shadow	Not Defined
Copy Provider	Not Defined
Net Logon	Not Defined
NetMeeting Remote Desktop Sharing	Not Defined
Network Connections	Not Defined
Network Dynamic Data Exchange (DDE)	Not Defined
Network DDE Share Database Manager (DSDM)	Not Defined
Network Location Awareness (NLA)	Not Defined
NT LM Security Support Provider	Not Defined
Performance Logs and Alerts	Not Defined
Plug and Play	Not Defined
Portable Media Serial Number Service	Not Defined
Print Spooler	Not Defined
Protected Storage	Not Defined
QoS RSVP	Not Defined
Remote Access Auto Connection Manager	Disabled
Remote Access Connection Manager	Disabled
Remote Desktop Help Session Manager	Disabled
Remote Procedure Call (RPC)	Not Defined

Remote Procedure Call (RPC) Locator	Not Defined
Remote Registry	Not Defined
Removable Storage Not defined	Not Defined
Routing and Remote Access	Disabled
Secondary Logon	Not Defined
Security Account Manager	Not Defined
Server	Not Defined
Shell Hardware	Not Defined
Detection	Not Defined
Smart Card	Not Defined
Smart Card Helper	Not Defined
Simple Mail Transfer	Not Defined
Protocol (SMTP)	Not Defined
Simple Network Management Protocol (SNMP) Service	Disabled
Simple Network Management Protocol (SNMP)Trap	Disabled
Simple Service Discovery Protocol discovery Service	Disabled
System Event Notification	Not Defined
System Restore Service	Not Defined
Task Scheduler Disabled	Disabled
TCP/IP NetBIOS Helper	Not Defined
Telephony	Not Defined
Telnet	Disabled
Terminal Services Disabled	Not Defined
Themes	Not Defined
Uninterruptable Power Supply	Not Defined
Upload Manager	Not Defined
Universal Plug and Play Device Host	Disabled
Volume Shadow Copy	Not Defined
WebClient	Not Defined
Windows Audio	Not Defined
Windows Image	Not Defined
Acquisition (WIA)	Not Defined
Windows Installer	Not Defined
Windows Management Instrumentation	Not Defined
Windows Management Instrumentation Driver Extensions	Not Defined
Windows Time	Not Defined
Wireless Zero	Disabled

Configuration	Not Defined
WMI Performance	Not Defined
Adapter Not defined	Not Defined
Workstation	Not Defined
World Wide Web Publishing Services	Disabled

8.4 Remote Access

The procedure for disabling the Remote Assistance and Remote Desktop features is different than disabling other services. Although these features are helpful for support, they also expose the computer to network-based attacks. As such, unless an organizational requirement exists to have them enabled, perform the following steps to disable them:

1. Right-click **My Computer** and select **Properties**.
2. Select the **Remote** tab and uncheck the **Allow Remote Assistance invitations to be sent from this computer** and **Allow users to connect remotely to this computer** boxes. Click **OK**.

9. Registry Keys

In order to implement adequate security in a Windows XP/2003 server environment, some registry key permissions should be changed. By default, permission to manipulate the registry is restricted, but because of the value of the registry, it is important to verify that the registry is protected. Following list is a recommended registry setting for security configuration. Permission on registry keys is set by default to Administrors full control, System Full Control, User Read.
Note: NSA/DISA set registry key permission but did not provide value for the keys.

Registry Keys	**Setting**
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg. Setting access permission to the registry	Administrator has Full Control, Backup Operators group has special permissions Query Value, Enumerate Subkeys, Notify, and Read Control, and LOCAL SERVICE has Read permissions
HKLM\Software\Microsoft \DrWatson\CreateCrashDump	0

Setting this value to 0 disables the creation of a memory dump file by the Dr. Watson program debugger.98 Memory dumps can contain sensitive information such as passwords. See Section 7.9 for additional information on suppressing memory dump file creation. This setting should be enabled to troubleshoot a recurring problem	
HKLM\Software\Microsoft \Windows NT\CurrentVersion\AEDebug\Auto Setting this value to 0 disables Dr. Watson.	0
HKLM\System\CurrentControlSet \Services\CDrom\Autorun Setting this value to 0 disables the autorun feature for CDs	0
HKLM\System\CurrentControlSet \Services\MrxSmb\Parameters \RefuseReset Setting this parameter to 1 causes the system to ignore ResetBrowser frames. Such frames can be used to shut down NetBIOS and master browsers and to declare a computer as being the new master browser. Earlier versions of Windows could be attacked through ResetBrowser frames.	1
HKLM\System\CurrentControlSet \Services\TCPIP\Parameters \EnablePMTUDiscovery When this parameter is set to 1, TCP attempts to discover the Maximum Transmission Unit (MTU), the size of the largest packet that can be kept intact over the path to a remote host. Setting this parameter to 0 disables the feature and causes an MTU of 576 bytes to be used for all connections that are not made to hosts on the local subnet.	Not defined

HKLM\System\CurrentControlSet \Services\TCPIP\Parameters \PerformRouterDiscovery This parameter controls whether the system attempts to perform router discovery per RFC 1256 on a per-interface basis. This feature should be disabled by setting the value to 0.	0
HKLM\System\CurrentControlSet \Services\TCPIP\Parameters \TcpMaxHalfOpen This setting specifies the number of connections permitted in the SYN-RCVD state before SynAttackProtect measures are implemented.	100
HKLM\System\CurrentControlSet \Services\TCPIP\Parameters \TcpMaxHalfOpenRetried This setting specifies the number of connections permitted in the SYN-RCVD state for which at least one retransmission of the SYN has been sent, before SynAttackProtect measures are implemented.	80
HKLM\System\CurrentControlSet \Services\TCPIP\Parameters \TCPMaxPortsExhausted This setting specifies how many connection requests can be refused before SynAttackProtect measures are implemented.	5
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ScreenSaverGracePeriod. This value sets the grace period between the activation of a password-protected screen saver and the requirement to enter a password to unlock the system. Setting this value to 0 eliminates the grace period.	0
HKLM\System\CurrentControlSet\Control\FileSystem\NtfsDisable8dot3NameCreation. Setting this value to 1 disables the automatic creation of legacy filenames in 8.3 format.	1

HKLM\System\CurrentControlSet\Control\Session Manager\SafeDllSearchMode. Windows XP searches directories in a particular order when it is looking for a file to execute. By default, Windows searches the current directory before the Windows and system directories. Setting this parameter to 1 causes Windows to search the Windows and system directories before searching the current directory. This is a better security practice because the current directory may be less restrictive than the Windows and system directories.	1
HKLM\System\CurrentControlSet\Services\EventLog\Security\WarningLevel. This value corresponds to a percentage of the maximum size of the security event log. When the security event log's size reaches the specified percentage, the system issues a warning.	80
HKLM\System\CurrentControlSet\Services\RasMan\Parameters\DisableSavePassword. Setting this parameter to 1 prevents the Network Connections phone book from saving passwords used for remote access.	1
HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\ NoDriveTypeAutoRun.94 The autorun feature attempts to run content from a CD automatically when it is placed in the system. If a CD contains malicious content, it could be automatically run. Setting this registry value to 255 disables the autorun feature for all types of drives.	255
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AutoAdminLogon. If enabled, this registry value allows the system login to be bypassed by using a password stored in cleartext within the registry. This password may be viewable by local users of the system. Also, an unauthorized party who gains physical access to the system may be able to gain access without providing any authentication. Setting the registry value to 0 disables the feature.	0
HKLM\System\CurrentControlSet\Control\CrashControl\AutoReboot. Enabling the AutoReboot feature causes the system to restart automatically after a failure or lockup. Some consider this to be undesirable from a security and operational standpoint.	0

10. Network Communication Ports

Windows XP/2003 Systems utilize network communication ports and systems services to provide wide variety of systems and network functions. As described in System services of this document, the recommended security configuration is to minimize the number of open ports and system services. Following table list a set of Windows system commonly used network ports.

10.1 Common Ports and Services

Port	Protocol	Service	Description
21	TCP	FTP	File
23	TCP	Telnet	Telnet service
68	UDP	DHCP	Dynamic Host Configuration Protocol client
80	TCP	HTTP	HyperText Transfer Protocol server
123	UDP	NTP	Network Time Protocol client (Windows Time)
135	TCP	epmap	DCE Endpoint Resolution (remote procedure call)
137	UDP	NetBIOS-ns	NetBIOS Name Service
138	UDP	NetBIOS-dgm	NetBIOS Datagram Service
139	TCP	NetBIOS-ssn	NetBIOS Session Service
161	UDP	SNMP	Simple Network Management Protocol
213	UDP	IPX	Over IP Client Service for Netware service
443	TCP	HTTPS	HTTP over SSL server
389	TCP/UDP	LDAP	Active Directory
445	TCP	UDP	microsoft-ds (SMB) Microsoft Common Internet File System (CIFS)
500	UDP	IKE	Internet Key Exchange (often used with IPsec)
515	TCP	LPR	Print Spooler service
522	TCP	NetMeeting	client178
636	TCP/UDP	LDAP SSL	Secure Channel for LDAP
1503	TCP	NetMeeting	client
1701	UDP	L2TP	Layer 2 Tunneling Protocol client
1720	TCP	NetMeeting	client
1723	TCP/UDP	PPTP	Point-to-Point Tunneling Protocol client
1731	TCP	NetMeeting	client
1900	UDP	SSDP	Simple Service Discovery Protocol
-2001			
2120			
UDP	Windows	Messenger	voice calls179
2869	TCP	UPnP	Universal Plug and Play
3002	TCP	Windows	Firewall/Sharing
3003	TCP	Windows	Firewall/Sharing
3389	TCP	RDP	Remote Desktop Protocol service
4500	UDP	L2TP/IPsec	NAT-T L2TP/IPSec
5000	TCP	UPnP	Universal Plug and Play
6801	UDP	Windows	voice calls

		Messenger	
-6891			
		Windows	
6900	TCP	Messenger	file transfers
		Windows	
6901	TCP/UDP	Messenger	voice calls

10.2 Stand Alone System

For standalone systems, the recommendation is to turn off the network interface from the operating system or from the bios of the PC.

10.3 Windows Firewall

For most applications, the Windows Firewall component provides adequate host-level protection against malicious inbound traffic. The Security Configuration Wizard (SCW) in Windows Server 2003 with SP1 greatly simplifies the setup and management of Windows Firewall settings for large deployments. IPsec should be used to secure host-to-host and host-client traffic where appropriate, and Windows Firewall should typically be widely deployed within most organizations as an additional defensive layer.

Note: There is no NISPOM requirement to set Window firewall. This firewall does not meet the CCVD EAL level required as a control interface.

10.4 Banner between network services

The recommendation for interactive connection between services of different machines should provide a banner to indicate the machine and the legal responsibilities. However, Some application services may not have the capabilities. However, Windows FTP and Telnet properties includes the ability to have Banner (see FTP site welcome property) displayed before login.

10.5 Disabling USB storage devices

The ability to use tiny USB memory sticks to download and walk away with relatively large amounts of data has already made the ubiquitous devices a potent security threat in the computing environment. Now, the emergence of USB flash drives that can store and automatically run applications straight off the device posses even more threat. The recommendation is to disable the USB storage device. This section describe two methods that can be used to prevent users from connecting to a USB storage device.

10.5.1 USB Storage Device Is Not Already Installed on the Computer

If a USB storage device is not already installed on the computer, assign the user or the group Deny permissions to the following files:

%SystemRoot%\Inf\Usbstor.pnf

%SystemRoot%\Inf\Usbstor.inf

When you do so, users cannot install a USB storage device on the computer. To assign a user or group Deny permissions to the Usbstor.pnf and Usbstor.inf files, follow these steps:
Start Windows Explorer, and then locate the %SystemRoot%\Inf folder

1. Right-click the **Usbstor.pnf** file, and then click **Properties**
2. Click the **Security** tab
3. In the **Group or user names** list, click the user or group that you want to set Deny permissions for.
4. In the **Permissions for *UserName or GroupName*** list, click to select the **Deny** check box next to **Full Control**, and then click **OK**.
   Note In addition, add the System account to the **Deny** list.
5. Right-click the **Usbstor.inf** file, and then click **Properties**.
6. Click the **Security** tab
7. In the **Group or user names** list, click the user or group that you want to set Deny permissions for.
8. In the **Permissions for *UserName or GroupName*** list, click to select the **Deny** check box next to **Full Control**, and then click **OK**

10.5.2 USB Storage Device Is Already Installed on the Computer

Warning Serious problems might occur if you modify the registry incorrectly by using Registry Editor or by using another method. These problems might require that you reinstall your operating system.

If a USB storage device is already installed on the computer, set the **Start** value in the following registry key to 4:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\UsbStor
When you do so, the USB storage device does not work when the user connects the device to the computer. To set the **Start** value, follow these steps:

1. Click **Start**, and then click **Run**
2. In the **Open** box, type **regedit**, and then click **OK**
3. Locate, and then click the following registry key:
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\UsbStor
4. In the right pane, double-click **Start**
5. In the **Value data** box, type **4**, click **Hexadecimal** (if it is not already selected), and then click **OK**.
6. Quit Registry Editor

10.5.3 USB Storage and System Events

When a USB storage device has been mounted, the system log will have an entry indicating the type of devices have been loaded. The event flags are Event ID 134/135/160 in the system event log, indicating USB storage device activity. The USB storage also creates a registry entry. See Registry entry in \CurrentControlSet\Enum\USBSTOR. These events require monitoring/auditing in meeting the NISPOM requirement for media controls and configuration management.

10.6 Disabling IPv6 protocol

IPv6 have mandated IPSec in its transport protocol, the compatibility issues usually forces the IPv6 being deployed without cryptography. The addition of IPsec in IPv6 does not affect the application layer. IPv6 ability to have multiple tunneling mechanisms allows unauthorized traffic to transit without knowing the source address. IPv6 benefits may out weight the security risk for implementing the protocol in some cases. The recommendation is to disable or uninstall IPv6 if not needed. Please note, some networking systems may require implementation of IPv6, such as firewall. In these implementations, the recommendation would be to include strong cryptography and filtering (such as RFC 2827 filtering) to avoid layer 4 spoofing.

IPv6 protocol for Windows XP with SP1 or later or Windows Server 2003 can be disabled by doing the following:

1. Log on to the computer with a user account that has privileges to change network configuration.
2. Click **Start**, click **Control Panel**, and then double-click **Network Connections**.
3. Right-click any local area connection, and then click **Properties**.
4. Click **Microsoft TCP/IP version 6** (for Windows XP with SP2 or later or Windows Server 2003) or **Microsoft IPv6 Developer Edition** (for Windows XP with SP1), and then click **Uninstall**.
5. When prompted to confirm the removal of the Microsoft IPv6 Developer Edition or Microsoft TCP/IP version 6 protocol, click **OK**.

Alternately, from the Windows XP or Windows Server 2003 desktop, click **Start**, point to **Programs**, point to **Accessories**, and then click **Command Prompt**. At the command prompt, type **netsh interface ipv6 uninstall**.

To remove the IPv6 protocol for Windows XP with no service packs installed, do the following:

Log on to the computer with a user account that has local administrator privileges.

From the Windows XP desktop, click **Start**, point to **Programs**, point to **Accessories**, and then click **Command Prompt**
At the command prompt, type **ipv6 uninstall**.

Alternately, from the Windows XP or Windows Server 2003 desktop, click **Start**, point to **Programs**, point to **Accessories**, and then click **Command Prompt**. At the command prompt, type **netsh interface ipv6 uninstall**.
To remove the IPv6 protocol for Windows XP with no service packs installed, do the following:

Add the following registry value (DWORD type) set to 0xFF:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters\
DisabledComponents

This method disables IPv6 on all your LAN interfaces, connections, and tunnel interfaces but does not disable the IPv6 loopback interface.

11. Conclusion

This document contains significant security settings that are available in Microsoft Windows Server 2003 with SP1 and Microsoft Windows XP Professional with SP2.
This document provided a summary of baseline technical security configuration standards for Window 200/XP/2003 systems. The document does not provide a complete step by step guide on how to set up the security. However, the implementation procedures for each component are described and provide a road map to the basic security configurations.

12. References

R. Bickel, et. al., Guide to Securing Microsoft Windows XP
National Security Agency, December 2003.

Murugiah Souppaya, Karen Kent, Paul M. Johnson,
Guidance for Securing Microsoft Windows XP Systems for IT
Professionals: A NIST Security Configuration Checklist, National Institute of Standards and Technology, October 2005

Microsoft Solutions for Security and Compliance Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP, Microsoft, January 2005.

MacDonald, Dave, Warren Barkley, "Microsoft Windows 2000 TCP/IP Implementation Details," white paper, http://secinf.net/info/nt/2000ip/tcpipimp.html.

McGovern, Owen, Julie Haney, *Guide to Securing Microsoft Windows 2000*, DISA and National Security Agency, May 2002.
Microsoft Technet, http://www.microsoft.com/technet.

Microsoft Windows XP Professional Resource Kit Documentation, Microsoft Press, 2001.