Defense Security Service
Office of the Designated
Approving Authority

Baseline Technical Security Configuration of Microsoft Windows 7 and Microsoft Server 2008 R2

Version 1.0
July 2013

Title Page

Document Name: Office of the Designated Approving Authority (ODAA) Baseline Technical Security Configuration for Microsoft Windows 7 and Windows Server 2008 R2

Publication Date: July 2013

Revision Date: N/A

Document Owner: Defense Security Service (DSS)
Industrial Security Field Operations (ISFO)
Office of the Designated Approving Authority (ODAA)

Point of Contact: Questions regarding the process or the figures provided should be directed to the Office of the Designated Approving Authority at ODAA@dss.mil.

Defense Security Service
Office of the Designated Approving Authority
Russell-Knox Building
27130 Telegraph Road
Quantico, VA 22134
www.dss.mil

Table of Contents

1.0 Introduction

The purpose of this document is to establish baseline technical configuration settings for securing the Microsoft Windows 7® and Microsoft Server 2008 R2 ® Operating Systems (OS) used in information systems (IS) accredited by the Defense Security Service (DSS) under the National Industrial Security Program (NISP). The protection of classified information maintained, hosted, or processed within IS necessitates the need for strong technical security controls to the maximum extent possible. The configuration settings described in this document are based on National Industrial Security Program Operating Manual (NISPOM) standards and on review and consideration by DSS of settings recommended by the Defense Information System Agency (DISA), National Institute of Standards and Technology (NIST), National Security Agency (NSA), Microsoft, Center for Internet Standards (CIS).

The use of the DSS baseline standards will strengthen system security controls and expedite DSS certification and accreditation (C&A) documentation reviews, as well as on-site verifications.

Although this document establishes the DSS recommended baseline configuration for Microsoft Windows 7® and Microsoft Server 2008 R2, DSS understands that due to unique operational environments some security controls or configuration settings may not be able to meet the baseline requirements found in this document, in which case contractors should address mitigation actions in the system security plan, or bring the matter to the attention of the assigned DSS Information System Security Professional (ISSP) to determine whether a valid variance exists or not and the need for pursuing a Risk Acceptance Letter (RAL).

2.0 General Assumptions

- Servers and Workstations are physically secured.
- General users do not have local administrative access.
- Every administrator (each person) has a separate account, i.e., no shared administrator accounts.
- Installation and patching is done OFF the network (to ensure a server is not exploited prior to patching.
- All drives are formatted NTFS.
- Routine functions and normal operating tasks (e.g. reading email) are not accomplished using privileged accounts.
- Remote access software will not be installed. Windows Terminal Services in application mode can be employed if non-administrators require remote console access.

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

If these assumptions are not true, contractor IS security personnel should document the reason for the exceptions in order to facilitate DSS staff performing certification and accreditation (C&A).

3.0 System Basics

- When assigning permissions to files and folders, replace Everyone Access Control Lists (ACL) 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 or application that requires a service account shall be documented in the Master System Security Plan (MSSP). Should the server be compromised, these accounts can easily be used to further compromise other domain systems. Pre-built code, easily obtainable on the Internet, can grab the password for service accounts (given a system level compromise). Service accounts must be set to fifteen characters and set to expire annually.
- IPSec is strongly encouraged for enhanced security if all client operating systems are capable.
- Consider implementing SMB signing and secure channel encryption if all clients have an Active Directory (AD) client.
- Systems shall be maintained at a Service Pack level supported by vendor with current security updates.

4.0 Group Policy Settings

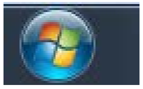
The following discusses those Group Policy (GP) settings that are applied at the Local and Domain Level. The built-in Default Domain Controller policy includes default setting values for these policies, which are collectively referred to as Account Policies.

The Group Policy settings can be created and edited by using the Group Policy Management Console (GPMC). The screen shots throughout the document represent examples of how to configure a system’s local GPMC. Client/Server environments will be enforced at the appropriate Organization Unit (OU) level.

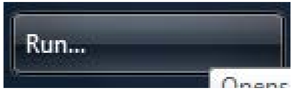
The baseline standards and settings provide a high level of security for Windows 7 systems when used in conjunction with a sound and comprehensive local security policy and other relevant security controls.

4.0.1 Launching Local Group Policy Editor

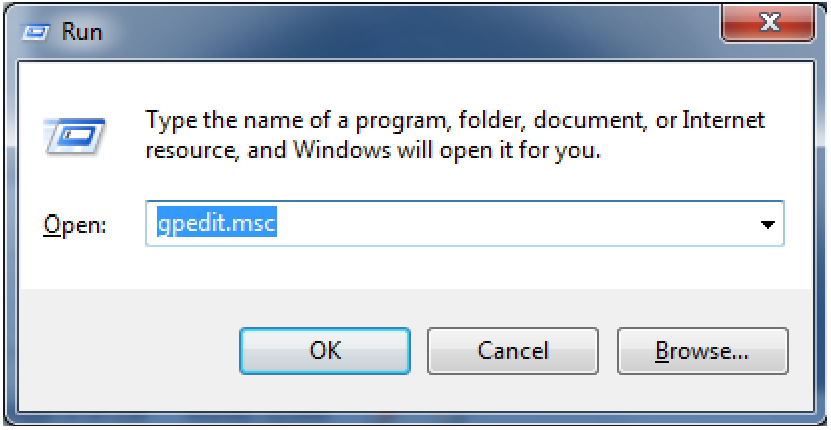
1.) Click Start



2.) Select Run



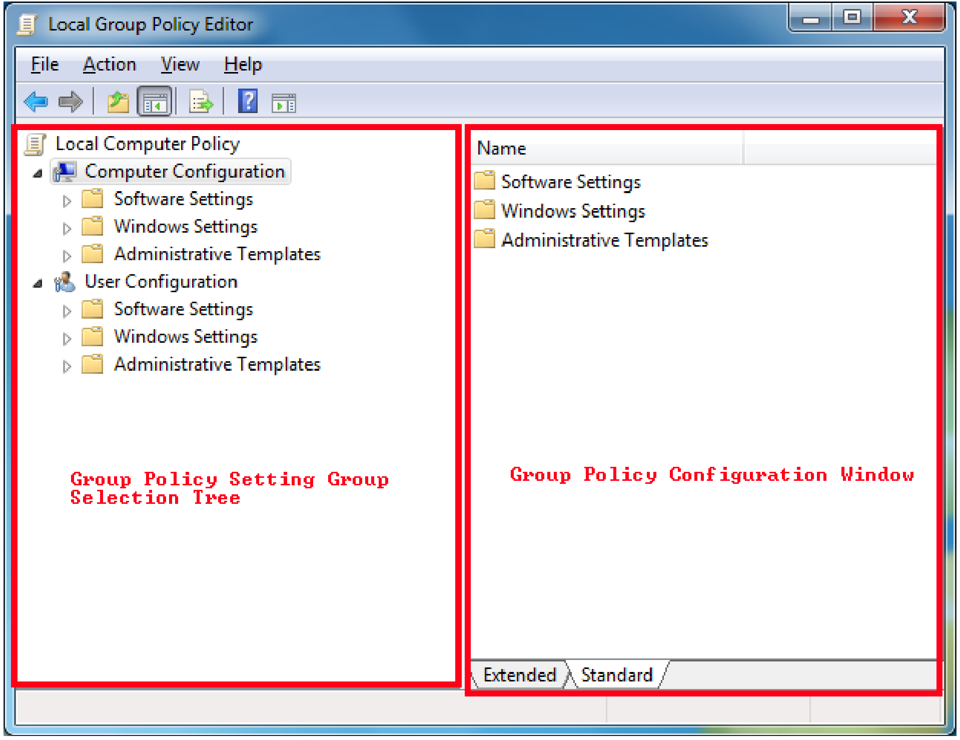
3.) Type “gpedit.msc” Click OK



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: gpedit.msc

Local Group Policy Editor



Group Policy Setting Group Selection Tree

Group Policy Configuration Window

4.1 Account Policies

There are three different types of account policies: password policies, account lockout policies, and Kerberos authentication policies. A single Microsoft Server 2008 domain may have one of each of these policies. If these policies are set at any other level in AD, only local accounts on member servers will be affected.

The account policy settings in GP are 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 configuring these policies in the AD 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 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 screen saver 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 apply.

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

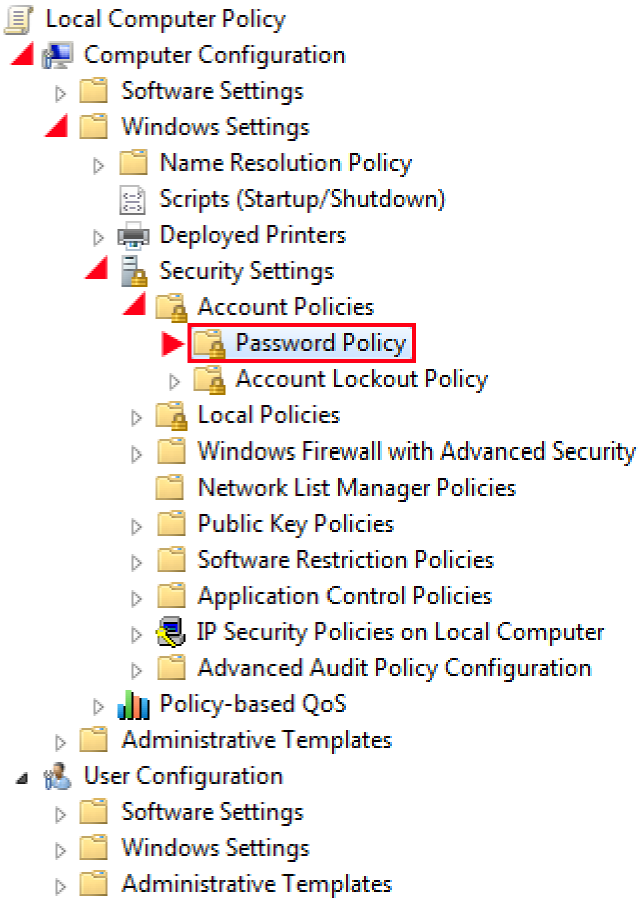
4.2 Password Policy

In Microsoft Windows and many other OS, the most common method to authenticate a user’s identity is to use a secret passphrase or password. A secure network environment requires all users to use strong passwords. 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.)

An appropriate password policy can enforce the use of strong passwords. Password policy settings control the complexity and lifetime of passwords. This section discusses each specific password policy account setting.

If groups exist that require separate password policies, they should be segmented into another domain or forest based on any additional requirements. Another option is to create fine-grained password policies by using Password Settings Object

GROUP POLICY : PASSWORD POLICY



- Local Computer Policy
  - Computer Configuration
    - Software Settings
    - Windows Settings
      - Name Resolution Policy
      - Scripts (Startup/Shutdown)
      - Deployed Printers
      - Security Settings
        - Account Policies
          - Password Policy
          - Account Lockout Policy
        - Local Policies
        - Windows Firewall with Advanced Security
        - Network List Manager Policies
        - Public Key Policies
        - Software Restriction Policies
        - Application Control Policies
        - IP Security Policies on Local Computer
        - Advanced Audit Policy Configuration
      - Policy-based QoS
    - Administrative Templates
  - User Configuration
    - Software Settings
    - Windows Settings
    - Administrative Templates

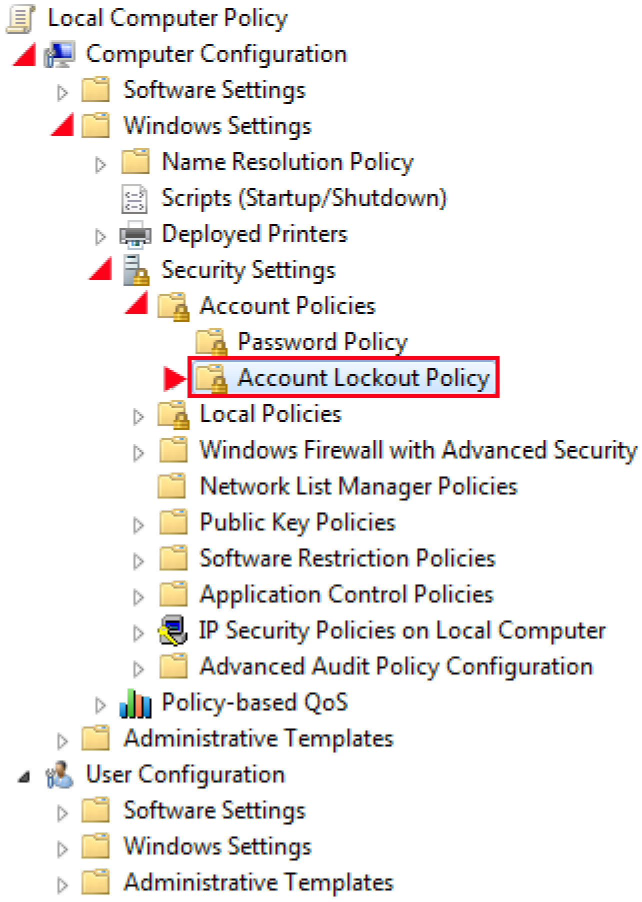
Setting	Value (MUSA,P2P,Client/Server)
Enforce password history	24
Maximum password age	60
Minimum password age	1 day
Minimum password length	14 character(s)
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

4.3 Account Lockout Policy

More than a few unsuccessful password submissions during an attempt to logon to a computer might represent an attacker's attempts to determine an account password by trial and error. The OS can be configured 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.

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.

GROUP POLICY : ACCOUNT LOCKOUT POLICY



- Local Computer Policy
  - Computer Configuration
    - Software Settings
    - Windows Settings
      - Name Resolution Policy
      - Scripts (Startup/Shutdown)
      - Deployed Printers
      - Security Settings
        - Account Policies
          - Password Policy
          - Account Lockout Policy
        - Local Policies
        - Windows Firewall with Advanced Security
        - Network List Manager Policies
        - Public Key Policies
        - Software Restriction Policies
        - Application Control Policies
        - IP Security Policies on Local Computer
        - Advanced Audit Policy Configuration
      - Policy-based QoS
    - Administrative Templates
  - User Configuration
    - Software Settings
    - Windows Settings
    - Administrative Templates

Setting	Value (MUSA, P2P, Client/Server)
Account lockout duration	0 minute(s)
Account lockout threshold	3 invalid logon attempt(s)
Reset account lockout counter after	60 minute(s)

4.4 Kerberos Policy

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 in a default installation of a Windows Server AD domain.

Since AD is necessary for Kerberos authentication, the Kerberos policies will not be defined in this document.

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. Both successful and failed attempts at actions can be audited.

The state of the OS and applications on a computer is dynamic. For example, security levels may be temporarily be 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.

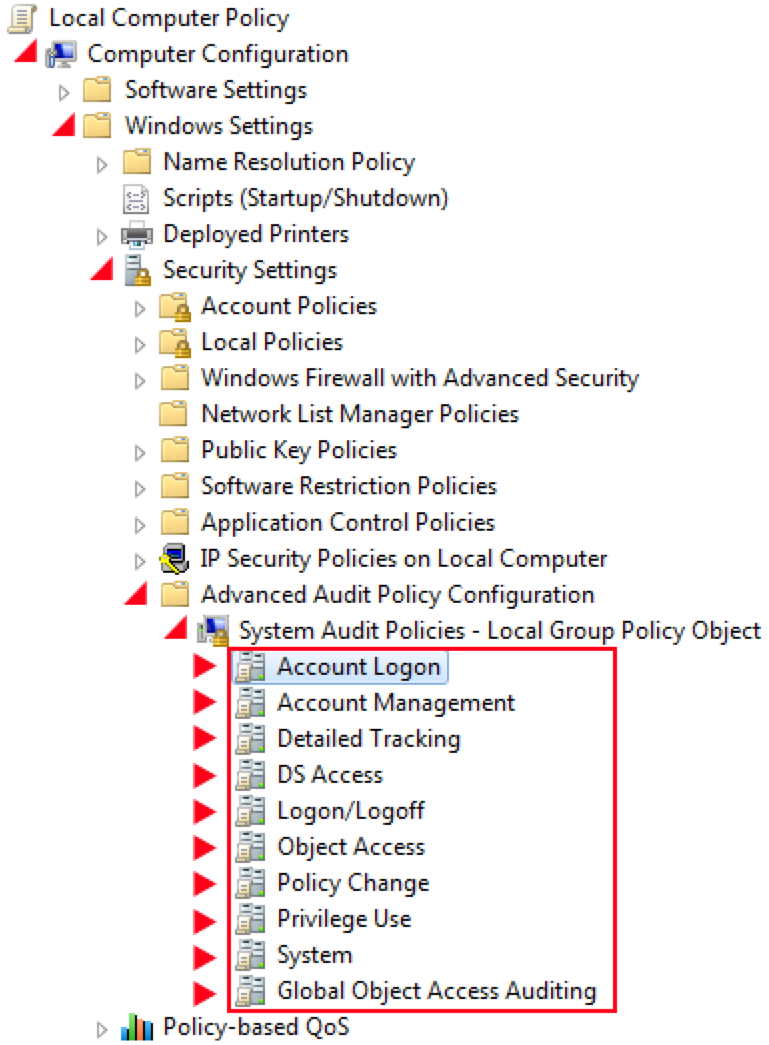
Regular security analyses enable administrators to track and determine that adequate security measures are in effect for each computer as part of an enterprise risk management program. Such analyses focus on highly specific information about all aspects of a computer that relate to security, which administrators can use to adjust the security levels. More importantly, this information can help detect any security flaws that may occur on 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 logon 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 OS, there are separate event logs for applications, security events, and system events. The security log records audit events. The event log container of GP 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.

Note: The familiar location for setting auditing in previous versions of Windows OS has changed in Windows 7 and Windows Server 2008 R2.

GROUP POLICY : ADVANCED AUDIT POLICIES



- Local Computer Policy
  - Computer Configuration
    - Software Settings
    - Windows Settings
      - Name Resolution Policy
      - Scripts (Startup/Shutdown)
      - Deployed Printers
      - Security Settings
        - Account Policies
        - Local Policies
        - Windows Firewall with Advanced Security
        - Network List Manager Policies
        - Public Key Policies
        - Software Restriction Policies
        - Application Control Policies
        - IP Security Policies on Local Computer
        - Advanced Audit Policy Configuration
          - System Audit Policies - Local Group Policy Object
            - Account Logon
            - Account Management
            - Detailed Tracking
            - DS Access
            - Logon/Logoff
            - Object Access
            - Policy Change
            - Privilege Use
            - System
            - Global Object Access Auditing
      - Policy-based QoS

Category	Setting	Value (MUSA, P2P,Client/Server)
Account Logon	Audit Credential Validation	Success and Failure
Account Logon	Audit Kerberos Authentication Service	No Auditing
Account Logon	Audit Kerberos Service Ticket Operations	No Auditing
Account Logon	Audit Other Account Logon Events	No Auditing
Account Management	Audit Application Group Management	No Auditing
Account Management	Audit Computer Account Management	Success and Failure
Account Management	Distribution Group Management	No auditing
Account Management	Other Account Management Events	Success and Failure
Account Management	Security Group Management	Success and Failure

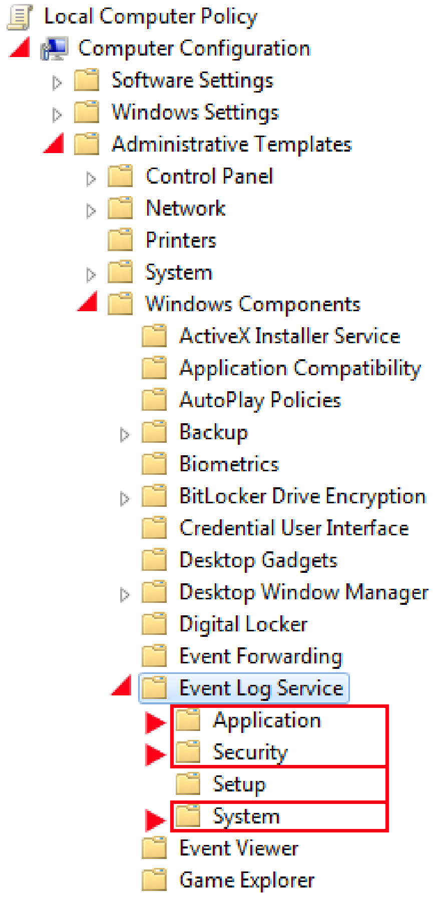
Category	Setting	Value (MUSA, P2P,Client/Server)
Account Management	User Account Management	Success and Failure
Detailed Tracking	DPAPI Activity	No auditing
Detailed Tracking	Process Creation	Success
Detailed Tracking	Process Termination	No auditing
Detailed Tracking	RPC Events	No Auditing
DS Access	Detailed Directory Service Replication	No Auditing
DS Access	Directory Service Access	Failure
DS Access	Directory Service Changes	No Auditing
DS Access	Directory Service Replication	No Auditing
Logon/Logoff	Account Lockout	No auditing
Logon/Logoff	IPsec Extended Mode	No auditing
Logon/Logoff	IPsec Main Mode	No auditing
Logon/Logoff	IPsec Quick Mode	No auditing
Logon/Logoff	Logoff	Success
Logon/Logoff	Logon	Success and Failure
Logon/Logoff	Network Policy Server	No auditing
Logon/Logoff	Other Logon/Logoff Events	No auditing
Logon/Logoff	Special Logon	Success
Object Access	Application Generated	No auditing
Object Access	Certification Services	No auditing
Object Access	Detailed File Share	No auditing
Object Access	File Share	No auditing
Object Access	File System	Failure
Object Access	Filtering Platform Connection	No auditing
Object Access	Filtering Platform Packet Drop	No auditing
Object Access	Handle Manipulation	No auditing
Object Access	Kernel Object	No auditing
Object Access	Other Object Access Events	No auditing
Object Access	Registry	Failure
Object Access	SAM	No auditing
Policy Change	Audit Policy Change	Success and Failure
Policy Change	Authentication Policy Change	Success
Policy Change	Authorization Policy Change	No auditing
Policy Change	Filtering Platform Policy Change	No auditing
Policy Change	MPSSVC Rule-Level Policy Change	No auditing
Policy Change	Other Policy Change Events	No auditing

Category	Setting	Value (MUSA, P2P,Client/Server)
Privilege Use	Non Sensitive Privilege Use	No auditing
Privilege Use	Other Privilege Use Events	No auditing
Privilege Use	Sensitive Privilege Use	Success and Failure
System	IPsec Driver	Success and Failure
System	Other System Events	No auditing
System	Security State Change	Success and Failure
System	Security System Extension	Success and Failure
System	System Integrity	Success and Failure

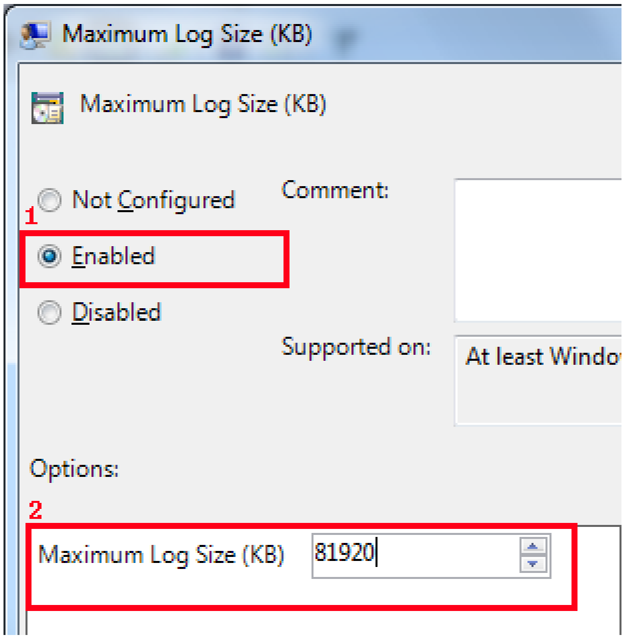
4.6 Event Log Configuration

The event log records events on the computer, and the security log records audit events. The event log container of the GP 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.

Group Policy | Event Log Service



- Local Computer Policy
  - Computer Configuration
    - Software Settings
    - Windows Settings
    - Administrative Templates
      - Control Panel
      - Network
      - Printers
      - System
      - Windows Components
        - ActiveX Installer Service
        - Application Compatibility
        - AutoPlay Policies
        - Backup
        - Biometrics
        - BitLocker Drive Encryption
        - Credential User Interface
        - Desktop Gadgets
        - Desktop Window Manager
        - Digital Locker
        - Event Forwarding
        - Event Log Service
          - Application
          - Security
          - Setup
          - System
        - Event Viewer
        - Game Explorer



Maximum Log Size (KB)

Maximum Log Size (KB)

○ Not Configured

● Enabled

○ Disabled

Comment:

Supported on: At least Windo

Options:

Maximum Log Size (KB) 81920

Figure 4.6.1

Category	Setting	Sub-Setting	(MUSA, P2P, Client/Server)
Application	Log File Path		Not Configured
Application	Maximum Log Size (KB)		Enabled
Application	Maximum Log Size (KB)	Maximum Log Size (KB)**	81920*
Application	Backup log automatically when full		Enabled
Application	Log Access		Enabled
Application	Retain old events		Disabled
Security	Log File Path		Not Configured
Security	Maximum Log Size (KB)		Enabled
Security	Maximum Log Size (KB)	Maximum Log Size (KB)**	81920*
Security	Backup log automatically when full		Enabled
Security	Log Access		Enabled
Security	Retain old events		Disabled
System	Log File Path		Not Configured
System	Maximum Log Size (KB)		Enabled
System	Maximum Log Size (KB)	Maximum Log Size (KB)**	81920*
System	Backup log automatically when full		Enabled
System	Log Access		Enabled
System	Retain old events		Disabled

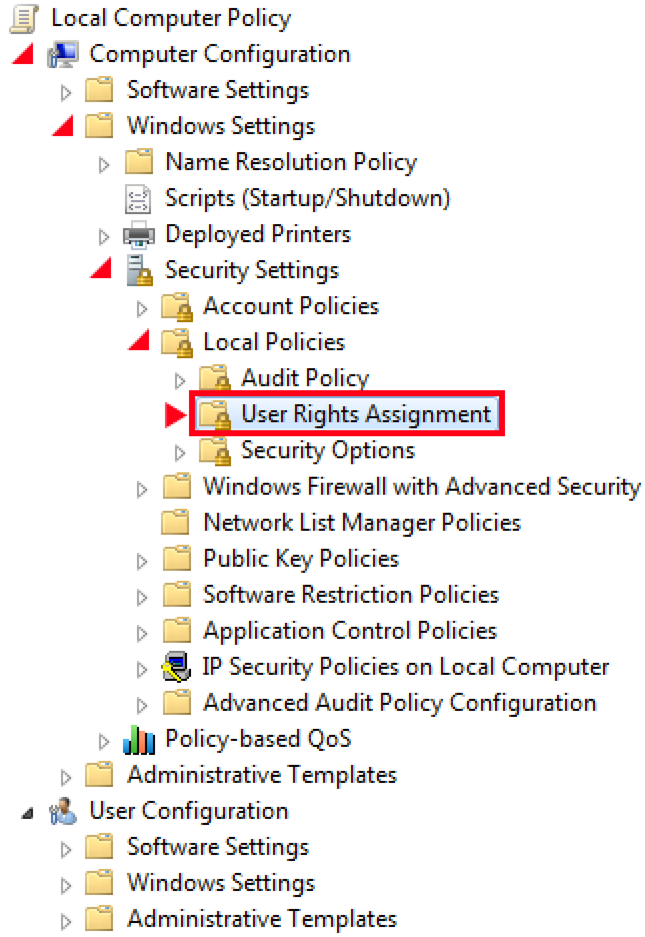
*Note: Log size may vary due to operational environment.
**Note: See Figure 4.6.1

4.7 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 logon to a computer. Privileges control access to computer and domain resources, and can override permissions that have been set on specific objects.

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.

Group Policy | User Rights Assignment



- Local Computer Policy
  - Computer Configuration
    - Software Settings
    - Windows Settings
      - Name Resolution Policy
      - Scripts (Startup/Shutdown)
      - Deployed Printers
      - Security Settings
        - Account Policies
        - Local Policies
          - Audit Policy
          - User Rights Assignment
          - Security Options
        - Windows Firewall with Advanced Security
        - Network List Manager Policies
        - Public Key Policies
        - Software Restriction Policies
        - Application Control Policies
        - IP Security Policies on Local Computer
        - Advanced Audit Policy Configuration
      - Policy-based QoS
    - Administrative Templates
  - User Configuration
    - Software Settings
    - Windows Settings
    - Administrative Templates

Setting	Value (MUSA, P2P, Client/Server)
Access Credential Manager as a trusted caller	No One
Access this computer from the network	Users, Administrators
Act as part of the operating system	No One

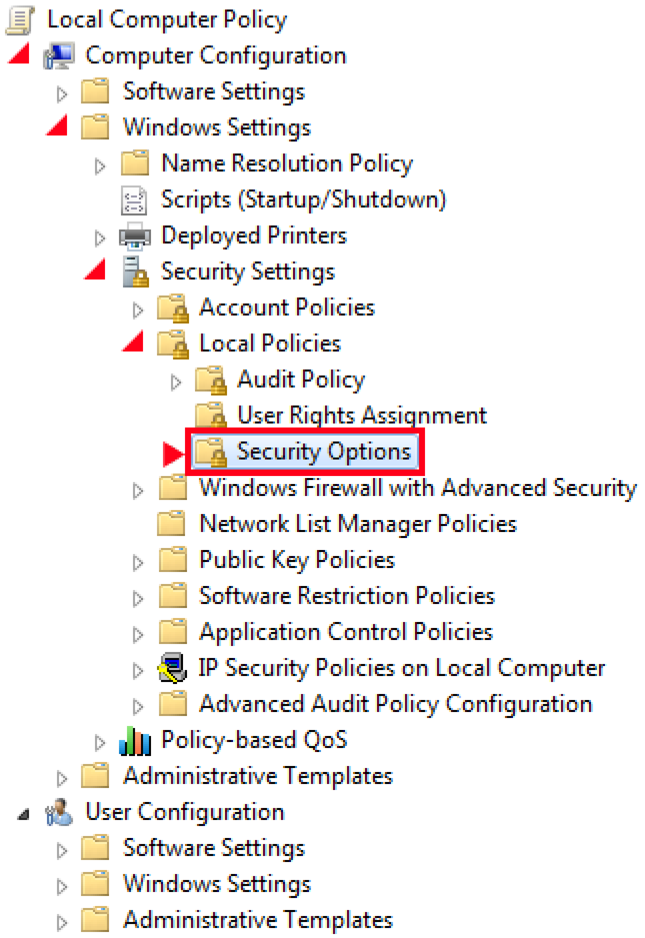
Setting	Value (MUSA, P2P, Client/Server)
Adjust memory quotas for a process	Administrators, Local Service, Network Service
Allow log on locally	Administrators, Authenticated Users
Allow log on through Remote Desktop Services	No One
Back up files and directories	Administrators
Bypass traverse checking	Users, Administrators
Change the system time	Administrators/Local Service
Change the time zone	Administrators, Users, Local Service
Create a pagefile	Administrators
Create a token object	No One
Create global objects	Administrators, Service, Local Service, Network Service Only
Create permanent shared objects	No One
Create symbolic links	Administrators
Debug programs	No One
Deny access to this computer from the network	Guests
Deny log on as a batch job	Guests
Deny log on as a service	No One
Deny log on locally	Guests
Deny log on through Remote Desktop Services	Everyone
Enable computer and user accounts to be trusted for delegation	No One
Force shutdown from a remote system	Administrators
Generate security audits	Local Service, Network Service
Impersonate a client after authentication	Administrators, SERVICE
Increase a process working set	Administrators, Local Service
Increase scheduling priority	Administrators, SERVICE
Load and unload device drivers	Administrators
Lock pages in memory	No One
Log on as a batch job	No One
Log on as a service	No One
Manage auditing and security log	Administrators, Auditors Group
Modify an object label	No One
Modify firmware environment values	Administrators

Setting	Value (MUSA, P2P, Client/Server)
Perform volume maintenance tasks	Administrators
Profile single process	Administrators
Profile system performance	Administrators, NT SERVICE\WdiServiceHost
Remove computer from docking station	Administrators, Users
Replace a process level token	Local Service, Network Service
Restore files and directories	Administrators
Shut down the system	Administrators, Users
Take ownership of files or other objects	Administrators

4.8 Security Options

The security options section of GP 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.

Group Policy | Security Options



- Local Computer Policy
  - Computer Configuration
    - Software Settings
    - Windows Settings
      - Name Resolution Policy
      - Scripts (Startup/Shutdown)
      - Deployed Printers
      - Security Settings
        - Account Policies
        - Local Policies
          - Audit Policy
          - User Rights Assignment
          - Security Options
        - Windows Firewall with Advanced Security
        - Network List Manager Policies
        - Public Key Policies
        - Software Restriction Policies
        - Application Control Policies
        - IP Security Policies on Local Computer
        - Advanced Audit Policy Configuration
      - Policy-based QoS
    - Administrative Templates
  - User Configuration
    - Software Settings
    - Windows Settings
    - Administrative Templates

Setting	MUSA	P2P	Client/Server
Accounts: Administrator account status	Disabled	Disabled	Disabled
Accounts: Guest account status	Disabled	Disabled	Disabled
Accounts: Limit local account use of blank passwords to console logon only	Enabled	Enabled	Enabled
Accounts: Rename administrator account	ORG DEFINED	ORG DEFINED	ORG DEFINED
Accounts: Rename guest account	ORG DEFINED	ORG DEFINED	ORG DEFINED
Audit: Audit the access of global system objects	Disabled	Disabled	Disabled

Setting	MUSA	P2P	Client/Server
Audit: Audit the use of Backup and Restore privilege	Disabled	Disabled	Disabled
Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings	Enabled	Enabled	Enabled
Audit: Shut down system immediately if unable to log security audits	Not Defined	Not Defined	Not Defined
DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL) syntax	Not Defined	Not Defined	Not Defined
DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDDL) syntax	Not Defined	Not Defined	Not Defined
Devices: Allow undock without having to log on	Disabled	Disabled	Disabled
Devices: Allowed to format and eject removable media	Administrators	Administrators	Administrators
Devices: Prevent users from installing printer drivers	Enabled	Enabled	Enabled
Devices: Restrict CD-ROM access to locally logged-on user only	Disabled	Disabled	Disabled
Devices: Restrict floppy access to locally logged-on user only	Disabled	Disabled	Disabled
Domain member: Digitally encrypt or sign secure channel data (always)	Not Defined	Not Defined	Enabled
Domain member: Digitally encrypt secure channel data (when possible)	Not Defined	Not Defined	Enabled
Domain member: Digitally sign secure channel data (when possible)	Not Defined	Not Defined	Enabled
Domain member: Disable machine account password changes	Disabled	Disabled	Disabled
Domain member: Maximum machine account password age	Not Defined	Not Defined	30 days
Domain member: Require strong (Windows 2000 or later) session key	Not Defined	Not Defined	Enabled
Interactive logon: Display user information when the session is locked.	Do not display user information	Do not display user information	Do not display user information
Interactive logon: Do not display last user name	Enabled	Enabled	Enabled
Interactive logon: Do not require CTRL+ALT+DEL	Disabled	Disabled	Disabled
Interactive logon: Message text for users attempting to log on (DoD Warning Banner for SIPRNET connected system only).	NISPOM Compliant Warning Banner (see note)	NISPOM Compliant Warning Banner (see note)	NISPOM Compliant Warning Banner (see note)

Setting	MUSA	P2P	Client/Server
Interactive logon: Message title for users attempting to log on	NISPOM Compliant Warning Banner	NISPOM Compliant Warning Banner	NISPOM Compliant Warning Banner
Interactive logon: Number of previous logons to cache (in case domain controller is not available)	Not defined	2 logons or less	2 logons or less
Interactive logon: Prompt user to change password before expiration	14 day(s)	14 day(s)	14 day(s)
Interactive logon: Require Domain Controller authentication to unlock workstation	Not Defined	Not Defined	Enabled
Interactive logon: Require smart card	Not defined	Not defined	Not defined
Interactive logon: Smart card removal behavior	Not defined	Not defined	Not defined
Microsoft network client: Digitally sign communications (always)	Not Defined	Enabled	Enabled
Microsoft network client: Digitally sign communications (if server agrees)	Not defined	Enabled	Enabled
Microsoft network client: Send unencrypted password to third-party SMB servers	Disabled	Disabled	Disabled
Microsoft network server: Amount of idle time required before suspending session	15 Minutes	15 Minutes	15 Minutes
Microsoft network server: Digitally sign communications (always)	Not defined	Enabled	Enabled
Microsoft network server: Digitally sign communications (if client agrees)	Not Defined	Enabled	Enabled
Microsoft network server: Disconnect clients when logon hours expire	Enabled	Enabled	Enabled
Microsoft network server: Server SPN target name validation level	Not defined	Accept if provided by client	Accept if provided by client
Network access: Allow anonymous SID/Name translation	Disabled	Disabled	Disabled
Network access: Do not allow anonymous enumeration of SAM accounts	Not Defined	Enabled	Enabled
Network access: Do not allow anonymous enumeration of SAM accounts and shares	Not Defined	Enabled	Enabled
Network access: Do not allow storage of passwords and credentials for network authentication	Not Defined	Enabled	Enabled
Network access: Let Everyone permissions apply to anonymous users	Disabled	Disabled	Disabled

Setting	MUSA	P2P	Client/Server
Network access: Named Pipes that can be accessed anonymously	Not Defined	Remove all entries. Legitimate applications may require entries to this registry value. If an application requires these entries to function properly document in the SSP.	Remove all entries. Legitimate applications may require entries to this registry value. If an application requires these entries to function properly document in the SSP.
Network access: Remotely accessible registry paths	Not Defined	Not Defined	Not Defined
Network access: Remotely accessible registry paths and sub-paths	Not Defined	Not Defined	Not Defined
Network access: Restrict anonymous access to Named Pipes and Shares	Not Defined	Enabled	Enabled
Network access: Shares that can be accessed anonymously	No entries	No entries	No entries
Network access: Sharing and security model for local accounts	Classic	Classic	Classic
Network security: Allow Local System to use computer identity for NTLM	Not Defined	Enabled	Enabled
Network security: Allow LocalSystem NULL session fallback	Disabled	Disabled	Disabled
Network Security: Allow PKU2U authentication requests to this computer to use online identities	Disabled	Disabled	Disabled
Network Security: Configure encryption types allowed for Kerberos	Not Defined	Enabled, set to RC4_HMAC_MD5, AES128_HMAC_SHA1, AES256_HMAC_SHA1, and Future Encryption Types	Enabled, set to RC4_HMAC_MD5, AES128_HMAC_SHA1, AES256_HMAC_SHA1, and Future Encryption Types
Network security: Do not store LAN Manager hash value on next password change	Not Defined	Enabled	Enabled
Network security: Force logoff when logon hours expire	Not Defined	Enabled	Enabled

Setting	MUSA	P2P	Client/Server
Network security: LAN Manager authentication level	Not Defined	Send NTLMv2 response only. Refuse LM & NTLM	Send NTLMv2 response only. Refuse LM & NTLM
Network security: LDAP client signing requirements	Not Defined	Require Signing	Require Signing
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients	Not Defined	Require NTLMv2 session security, Require 128-bit encryption	Require NTLMv2 session security, Require 128-bit encryption
Network security: Minimum session security for NTLM SSP based (including secure RPC) servers	Not Defined	Require NTLMv2 session security, Require 128-bit encryption	Require NTLMv2 session security, Require 128-bit encryption
Network Security: Restrict NTLM: Add remote server exceptions for NTLM authentication	Not defined	Not defined	Not defined
Network Security: Restrict NTLM: Add server exceptions in this domain	Not defined	Not defined	Not defined
Network Security: Restrict NTLM: Audit Incoming NTLM Traffic	Not defined	Not defined	Not defined
Network Security: Restrict NTLM: Audit NTLM authentication in this domain	Not defined	Not defined	Not defined
Network Security: Restrict NTLM: Incoming NTLM traffic	Not defined	Not defined	Not defined
Network Security: Restrict NTLM: NTLM authentication in this domain	Not defined	Not defined	Not defined
Network Security: Restrict NTLM: Outgoing NTLM traffic to remote servers	Not defined	Not defined	Not defined
Recovery console: Allow automatic administrative logon	Disabled	Disabled	Disabled
Recovery console: Allow floppy copy and access to all drives and all folders	Disabled	Disabled	Disabled

Setting	MUSA	P2P	Client/Server
Shutdown: Allow system to be shut down without having to log on	Enabled	Enabled	Disabled
Shutdown: Clear virtual memory pagefile	Disabled	Disabled	Disabled
System cryptography: Force strong key protection for user keys stored on the computer	Not defined	Not defined	Set to: User must enter a password each time they use a key
System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing	Not Defined	Enabled	Enabled
System objects: Require case insensitivity for non-Windows subsystems	Enabled	Enabled	Enabled
System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)	Enabled	Enabled	Enabled
System settings: Optional subsystems	No entries	No entries	No entries
System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies	Enabled	Enabled	Enabled
User Account Control: Admin Approval Mode for the Built-in Administrator account	Enabled	Enabled	Enabled
User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop	Not Defined	Disabled	Disabled
User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode	Prompt for consent on the secure desktop	Prompt for consent on the secure desktop	Prompt for consent on the secure desktop
User Account Control: Behavior of the elevation prompt for standard users	Prompt for credentials on the secure desktop	Prompt for credentials on the secure desktop	Prompt for credentials on the secure desktop
User Account Control: Detect application installations and prompt for elevation	Enabled	Enabled	Enabled
User Account Control: Only elevate executables that are signed and validated	Disabled	Disabled	Disabled
User Account Control: Only elevate UIAccess applications that are installed in secure locations	Enabled	Enabled	Enabled
User Account Control: Run all administrators in Admin Approval Mode	Enabled	Enabled	Enabled

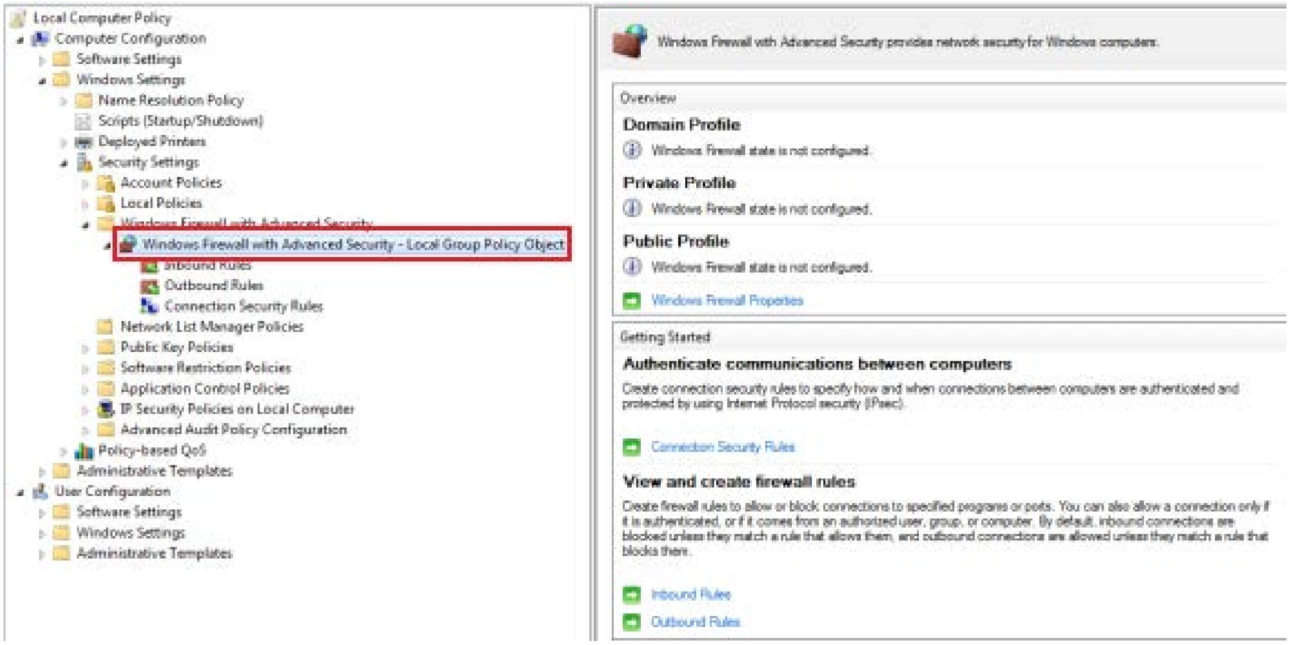
Setting	MUSA	P2P	Client/Server
User Account Control: Switch to the secure desktop when prompting for elevation	Enabled	Enabled	Enabled
User Account Control: Virtualize file and registry write failures to per-user locations	Enabled	Enabled	Enabled

4.9 Windows Firewall

A firewall is software or hardware that checks information coming from the Internet or a network, and then either blocks or allows it to pass through to the computer, depending on the firewall settings.

A firewall can help prevent hackers or malicious software (such as worms) from gaining access to the computer through a network or the Internet. A firewall can also help stop the computer from sending malicious software to other computers.

Group Policy | Windows Firewall



Windows Firewall with Advanced Security provides network security for Windows computers.

Overview

Domain Profile

Windows Firewall state is not configured.

Private Profile

Windows Firewall state is not configured.

Public Profile

Windows Firewall state is not configured.

Windows Firewall Properties

Getting Started

Authenticate communications between computers

Create connection security rules to specify how and when connections between computers are authenticated and protected by using Internet Protocol security (IPsec).

Connection Security Rules

View and create firewall rules

Create firewall rules to allow or block connections to specified programs or ports. You can also allow a connection only if it is authenticated, or if it comes from an authorized user, group, or computer. By default, inbound connections are blocked unless they match a rule that allows them, and outbound connections are allowed unless they match a rule that blocks them.

Inbound Rules

Outbound Rules

Setting	UI Path	MUSA	P2P	Client/Server
Enable Firewall	Configure the policy value for Computer Configuration \Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\ Windows Firewall Properties (this link will be in the right pane) **Domain Profile Tab** \State, "Firewall State" to "On (recommended)".	Note defined	On	On
Enable Firewall	Configure the policy value for Computer Configuration \Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\ Windows Firewall Properties (this link will be in the right pane) **Private Profile** \State, "Firewall State" to "On (recommended)".	Note defined	On	On
Enable Firewall	Configure the policy value for Computer Configuration \Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\ Windows Firewall Properties (this link will be in the right pane) **Public Profile** \State, "Firewall State" to "On (recommended)".	Note defined	On	On
Block Unsolicited inbound connections	Configure the policy value for Computer Configuration Windows Settings\ Security Settings\ Windows Firewall with Advanced Security \ Windows Firewall with Advanced Security \ Windows Firewall Properties (this link will be in the right pane) \ **Domain Profile Tab** **->** State, "Inbound Connections" to "Block (default)".	Note defined	Block (default)	Block (default)
Allow Outbound Connections	Configure the policy value for Computer Configuration Windows Settings \ Security Settings \ Windows Firewall with Advanced Security \ Windows Firewall with Advanced Security\ Windows Firewall Properties (this link will be in the right pane) \ **Domain Profile Tab** \ State, "Outbound Connections" to "Allow (default)".	Note defined	Allow (default)	Allow (default)

Setting	UI Path	MUSA	P2P	Client/Server
Display Notifications	Configure the policy value for Computer Configuration Windows Settings \ Security Settings \ Windows Firewall with Advanced Security \ Windows Firewall with Advanced Security \ Windows Firewall Properties (this link will be in the right pane) \ **Domain Profile Tab** \ Settings (select Customize) \ Firewall settings, “Display a notification” to “Yes (default)”	Note defined	Display a notification” to “Yes (default)”	Display a notification” to “Yes (default)”
Unicast Response	Configure the policy value for Computer Configuration Windows Settings \ Security Settings \ Windows Firewall with Advanced Security \ Windows Firewall with Advanced Security \ Windows Firewall Properties (this link will be in the right pane) \ **Domain Profile Tab** \ Settings (select Customize) \ Unicast response, “Allow unicast response” to “No”	Note defined	Allow unicast response” to “No	Allow unicast response” to “No
Local Firewall Rules	Configure the policy value for Computer Configuration Windows Settings \ Security Settings \ Windows Firewall with Advanced Security \ Windows Firewall with Advanced Security \ Windows Firewall Properties (this link will be in the right pane) \ **Domain Profile Tab** \ Settings (select Customize) \ Rule merging, “Apply local firewall rules” to “No”	Note defined	Apply local firewall rules” to “No	Apply local firewall rules” to “No
Local Connection Rules	Configure the policy value for Computer Configuration Windows Settings \ Security Settings\ Windows Firewall with Advanced Security \ Windows Firewall with Advanced Security\ Windows Firewall Properties (this link will be in the right pane) \ **Domain Profile Tab** \ Settings (select Customize) -\ Rule merging, “Apply local connection security rules” to “No”	Note defined	Apply local connection security rules” to “No”	Apply local connection security rules” to “No”
Log File	Configure the policy value for Computer Configuration Windows Settings \ Security Settings \ Windows Firewall with Advanced Security \ Windows Firewall with Advanced Security\ Windows Firewall Properties (this link will be in the right pane) \ **Domain Profile Tab** \ Logging (select Customize), “Name” to “%windir%.log”.	Note defined	Name” to “%windir%.log	Name” to “%windir%.log

Setting	UI Path	MUSA	P2P	Client/Server
Log Size	Configure the policy value for Computer Configuration Windows Settings \ Security Settings \ Windows Firewall with Advanced Security \ Windows Firewall with Advanced Security\ Windows Firewall Properties (this link will be in the right pane) \ **Domain Profile Tab** \ Logging (select Customize), “Size limit (KB):” to “16,384” (or greater)	Note defined	Size limit (KB):” to “16,384” (or greater)	Size limit (KB):” to “16,384” (or greater)
Log Dropped Packets	Configure the policy value for Computer Configuration Windows Settings \ Security Settings \ Windows Firewall with Advanced Security \ Windows Firewall with Advanced Security\ Windows Firewall Properties (this link will be in the right pane) \ **Domain Profile Tab** \ Logging (select Customize), “Log dropped packets” to “Yes”	Note defined	“Log dropped packets” to “Yes”	“Log dropped packets” to “Yes”
Log Successful Connections	Configure the policy value for Computer Configuration Windows Settings \ Security Settings \ Windows Firewall with Advanced Security \ Windows Firewall with Advanced Security\ Windows Firewall Properties (this link will be in the right pane) \ **Domain Profile Tab** \ Logging (select Customize), “Log successful connections” to “Yes”	Note defined	“Log successful connections” to “Yes”	“Log successful connections” to “Yes”
Block Unsolicited inbound connections	Configure the policy value for Computer Configuration Windows Settings\ Security Settings\ Windows Firewall with Advanced Security \ Windows Firewall with Advanced Security \ Windows Firewall Properties (this link will be in the right pane) \ **Private Profile Tab** -> State, “Inbound Connections” to “Block (default)”.	Not defined	Block (default)	Block (default)
Allow Outbound Connections	Configure the policy value for Computer Configuration Windows Settings \ Security Settings \ Windows Firewall with Advanced Security \ Windows Firewall with Advanced Security\ Windows Firewall Properties (this link will be in the right pane) \ **Private Profile Tab** \ State, “Outbound Connections” to “Allow (default)”.	Not defined	Allow (default)	Allow (default)

Setting	UI Path	MUSA	P2P	Client/Server
Display Notifications	Configure the policy value for Computer Configuration Windows Settings \ Security Settings \ Windows Firewall with Advanced Security \ Windows Firewall with Advanced Security \ Windows Firewall Properties (this link will be in the right pane) \ **Private Profile Tab** \ Settings (select Customize) \ Firewall settings, “Display a notification” to “Yes (default)”	Note defined	Display a notification” to “Yes (default)”	Display a notification” to “Yes (default)”
Unicast Response	Configure the policy value for Computer Configuration Windows Settings \ Security Settings \ Windows Firewall with Advanced Security \ Windows Firewall with Advanced Security \ Windows Firewall Properties (this link will be in the right pane) \ **Private Profile Tab** \ Settings (select Customize) \ Unicast response, “Allow unicast response” to “No”	Not defined	Allow unicast response” to “No	Allow unicast response” to “No
Local Firewall Rules	Configure the policy value for Computer Configuration Windows Settings \ Security Settings \ Windows Firewall with Advanced Security \ Windows Firewall with Advanced Security \ Windows Firewall Properties (this link will be in the right pane) \ **Private Profile Tab** \ Settings (select Customize) \ Rule merging, “Apply local firewall rules” to “No”	Not defined	Apply local firewall rules” to “No	Apply local firewall rules” to “No
Local Connection Rules	Configure the policy value for Computer Configuration Windows Settings \ Security Settings\ Windows Firewall with Advanced Security \ Windows Firewall with Advanced Security\ Windows Firewall Properties (this link will be in the right pane) \ **Private Profile Tab** \ Settings (select Customize) -\ Rule merging, “Apply local connection security rules” to “No”	Not defined	Apply local connection security rules” to “No”	Apply local connection security rules” to “No”
Log File	Configure the policy value for Computer Configuration Windows Settings \ Security Settings \ Windows Firewall with Advanced Security \ Windows Firewall with Advanced Security\ Windows Firewall Properties (this link will be in the right pane) \ **Private Profile Tab** \ Logging (select Customize), “Name” to “%windir%.log”.	Not defined	Name” to “%windir%.log	Name” to “%windir%.log

Setting	UI Path	MUSA	P2P	Client/Server
Log Size	Configure the policy value for Computer Configuration Windows Settings \ Security Settings \ Windows Firewall with Advanced Security \ Windows Firewall with Advanced Security\ Windows Firewall Properties (this link will be in the right pane) \ **Private Profile Tab** \ Logging (select Customize), “Size limit (KB):” to “16,384” (or greater)	Not defined	Size limit (KB):” to “16,384” (or greater)	Size limit (KB):” to “16,384” (or greater)
Log Dropped Packets	Configure the policy value for Computer Configuration Windows Settings \ Security Settings \ Windows Firewall with Advanced Security \ Windows Firewall with Advanced Security\ Windows Firewall Properties (this link will be in the right pane) \ **Private Profile Tab** \ Logging (select Customize), “Log dropped packets” to “Yes”	Not defined	“Log dropped packets” to “Yes”	“Log dropped packets” to “Yes”
Log Successful Connections	Configure the policy value for Computer Configuration Windows Settings \ Security Settings \ Windows Firewall with Advanced Security \ Windows Firewall with Advanced Security\ Windows Firewall Properties (this link will be in the right pane) \ **Private Profile Tab** \ Logging (select Customize), “Log successful connections” to “Yes”	Not defined	“Log successful connections” to “Yes”	“Log successful connections” to “Yes”
Block Unsolicited inbound connections	Configure the policy value for Computer Configuration Windows Settings\ Security Settings\ Windows Firewall with Advanced Security \ Windows Firewall with Advanced Security \ Windows Firewall Properties (this link will be in the right pane) \ **Public Profile Tab** -> State, “Inbound Connections” to “Block (default)”.	Not defined	Block (default)	Block (default)
Allow Outbound Connections	Configure the policy value for Computer Configuration Windows Settings \ Security Settings \ Windows Firewall with Advanced Security \ Windows Firewall with Advanced Security\ Windows Firewall Properties (this link will be in the right pane) \ **Public Profile Tab** \ State, “Outbound Connections” to “Allow (default)”.	Not defined	Allow (default)	Allow (default)

Setting	UI Path	MUSA	P2P	Client/Server
Display Notifications	Configure the policy value for Computer Configuration Windows Settings \ Security Settings \ Windows Firewall with Advanced Security \ Windows Firewall with Advanced Security \ Windows Firewall Properties (this link will be in the right pane) \ **Public Profile Tab** \ Settings (select Customize) \ Firewall settings, “Display a notification” to “Yes (default)”	Note defined	Display a notification” to “Yes (default)”	Display a notification” to “Yes (default)”
Unicast Response	Configure the policy value for Computer Configuration Windows Settings \ Security Settings \ Windows Firewall with Advanced Security \ Windows Firewall with Advanced Security \ Windows Firewall Properties (this link will be in the right pane) \ **Public Profile Tab** \ Settings (select Customize) \ Unicast response, “Allow unicast response” to “No”	Not defined	Allow unicast response” to “No	Allow unicast response” to “No
Local Firewall Rules	Configure the policy value for Computer Configuration Windows Settings \ Security Settings \ Windows Firewall with Advanced Security \ Windows Firewall with Advanced Security \ Windows Firewall Properties (this link will be in the right pane) \ **Public Profile Tab** \ Settings (select Customize) \ Rule merging, “Apply local firewall rules” to “No”	Not defined	Apply local firewall rules” to “No	Apply local firewall rules” to “No
Local Connection Rules	Configure the policy value for Computer Configuration Windows Settings \ Security Settings\ Windows Firewall with Advanced Security \ Windows Firewall with Advanced Security\ Windows Firewall Properties (this link will be in the right pane) \ **Public Profile Tab** \ Settings (select Customize) -\ Rule merging, “Apply local connection security rules” to “No”	Not defined	Apply local connection security rules” to “No”	Apply local connection security rules” to “No”
Log File	Configure the policy value for Computer Configuration Windows Settings \ Security Settings \ Windows Firewall with Advanced Security \ Windows Firewall with Advanced Security\ Windows Firewall Properties (this link will be in the right pane) \ **Public Profile Tab** \ Logging (select Customize), “Name” to “%windir%.log”.	Not defined	Name” to “%windir%.log	Name” to “%windir%.log

Setting	UI Path	MUSA	P2P	Client/Server
Log Size	Configure the policy value for Computer Configuration Windows Settings \ Security Settings \ Windows Firewall with Advanced Security \ Windows Firewall with Advanced Security\ Windows Firewall Properties (this link will be in the right pane) \ **Public Profile Tab** \ Logging (select Customize), “Size limit (KB):” to “16,384” (or greater)	Not defined	Size limit (KB):” to “16,384” (or greater)	Size limit (KB):” to “16,384” (or greater)
Log Dropped Packets	Configure the policy value for Computer Configuration Windows Settings \ Security Settings \ Windows Firewall with Advanced Security \ Windows Firewall with Advanced Security\ Windows Firewall Properties (this link will be in the right pane) \ **Public Profile Tab** \ Logging (select Customize), “Log dropped packets” to “Yes”	Not defined	“Log dropped packets” to “Yes”	“Log dropped packets” to “Yes”
Log Successful Connections	Configure the policy value for Computer Configuration Windows Settings \ Security Settings \ Windows Firewall with Advanced Security \ Windows Firewall with Advanced Security\ Windows Firewall Properties (this link will be in the right pane) \ **Public Profile Tab** \ Logging (select Customize), “Log successful connections” to “Yes”	Not defined	“Log successful connections” to “Yes”	“Log successful connections” to “Yes”

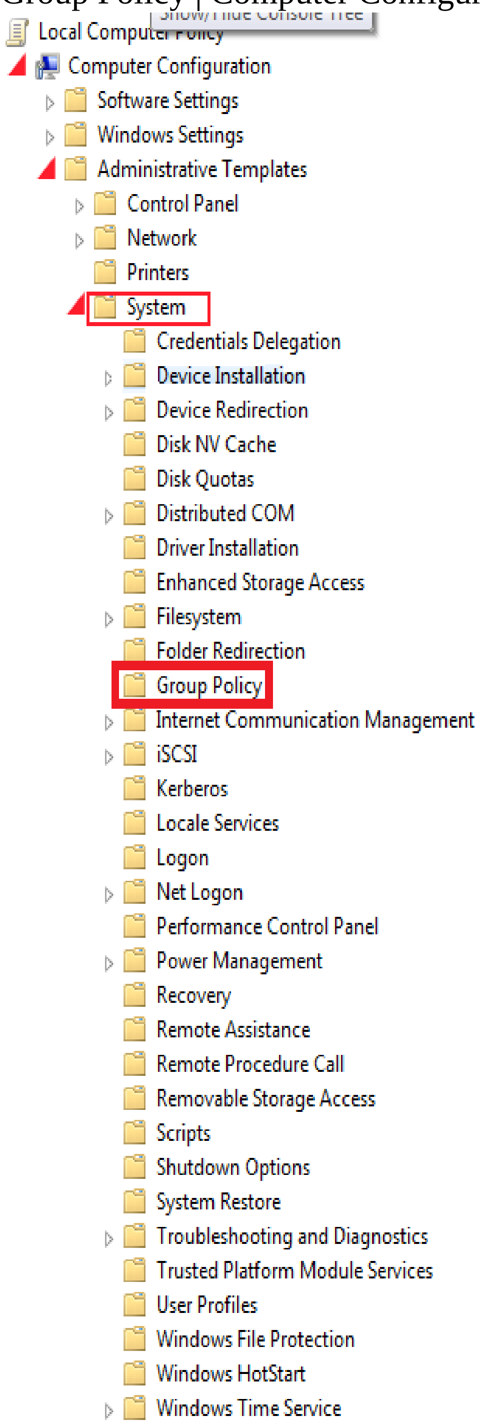
Setting	UI Path	MUSA	P2P	Client/Server
IPv6 Block Protocols 41	Computer Configuration Windows Settings \ Security Settings \ Windows Firewall with Advanced Security \ Windows Firewall with Advanced Security\ Outbound Rules "IPv6 Block of Protocols 41" will be configured as follows: **Add the rule with the following steps**: Navigate to Outbound Rules. Right click in right pane and select "New Rule". Select "Custom", Next. Select "All Programs", Next. Select Protocol Type: IPv6 (Protocol number 41 will be automatically selected). Select "Any IP address" for both local and remote IP address this rule will match. Next. Select "Block the connection", Next. Select all (Domain, Private and Public) for When does this rule apply? Next. Supply the Name: IPv6 Block of Protocols 41. Finish.	Not defined	Add "IPv6 Block of Protocols 41" Rule	Add "IPv6 Block of Protocols 41" Rule

Setting	UI Path	MUSA	P2P	Client/Server
IPv6 Block UDP 3544	Computer Configuration Windows Settings \ Security Settings \ Windows Firewall with Advanced Security \ Windows Firewall with Advanced Security\ Outbound Rules “IPv6 Block of UDP 3544” will be configured as follows: Add the rule with the following steps: Navigate to Outbound Rules. Right click in right pane and select “New Rule”. Select “Port”, Next. Select “All Programs”, Next. Select Protocol Type: UDP. Select Local Port: Specific Ports, Enter 3544. Select Remote Port: All Ports, Next. Select “Any IP address” for both local and remote IP address this rule will match. Next. Select “Block the connection”, Next. Select all (Domain, Private and Public) for When does this rule apply? Next. Supply the Name: IPv6 Block of UDP 3544. Finish.	Not defined	Add “IPv6 Block of UDP 3544” Rule	Add “IPv6 Block of UDP 3544” Rule

4.10 Group Policy Processing

The following section covers group policy processing settings.

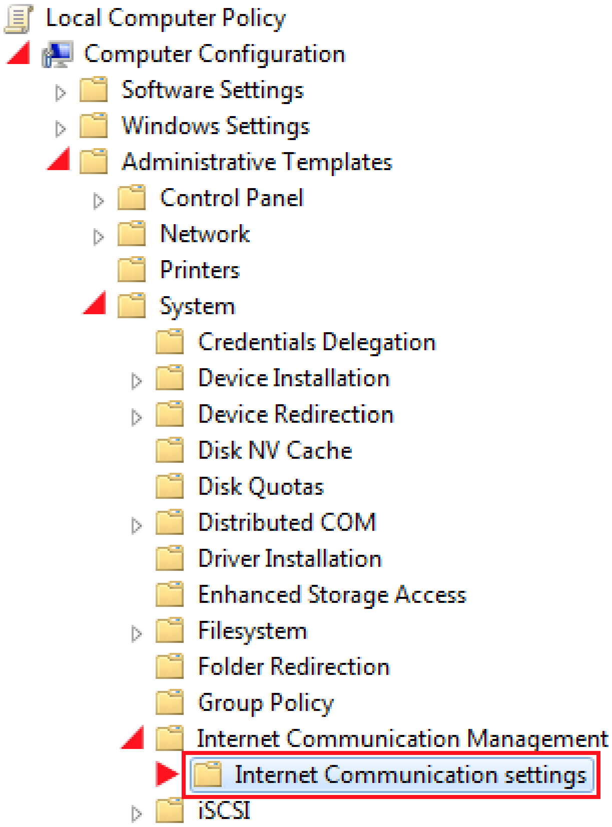
Group Policy | Computer Configuration > Administrative Templates > System



Computer Configuration > Administrative Templates > System >Group Policy

Category	Setting	MUSA	P2P	Client/Server
Group Policy	Registry policy processing	Not Defined	Not Defined	Enabled
	Do not apply during periodic background processing			False
	Process even if the Group Policy objects have not changed			True

4.11 Internet Communication Settings



- Local Computer Policy
  - Computer Configuration
    - Software Settings
    - Windows Settings
    - Administrative Templates
      - Control Panel
      - Network
      - Printers
      - System
        - Credentials Delegation
        - Device Installation
        - Device Redirection
        - Disk NV Cache
        - Disk Quotas
        - Distributed COM
        - Driver Installation
        - Enhanced Storage Access
        - Filesystem
        - Folder Redirection
        - Group Policy
        - Internet Communication Management
          - Internet Communication settings
        - iSCSI

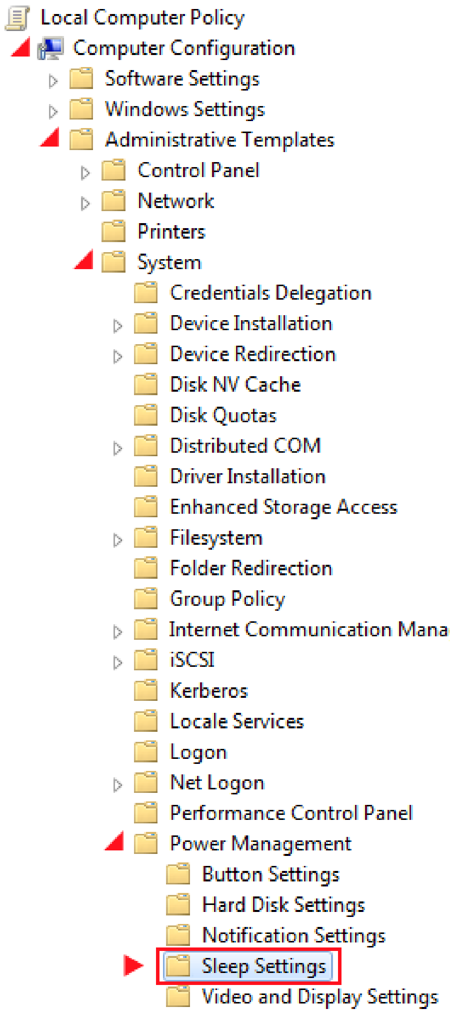
Setting	MUSA, P2P, Client/Server
Turn off downloading of print drivers over HTTP	Enabled
Turn off Internet download for Web publishing and online ordering wizards	Enabled
Turn off printing over HTTP	Enabled
Turn off Search Companion content file updates	Enabled
Turn off the "Publish to Web" task for files and folders	Enabled
Turn off the Windows Messenger Customer Experience Improvement Program	Enabled
Turn off Windows Update device driver searching	Enabled

4.12 Run at Logon Settings

Computer Configuration > Administrative Templates> System > Logon

Setting	MUSA, P2P, Client/Server
Do not process the legacy run list	Not Defined
Do not process the run once list	Not Defined

4.13 Power Management



Setting	MUSA, P2P, Client/Server
Require a Password When a Computer Wakes (On Battery)	Enabled
Require a Password When a Computer Wakes (Plugged In)	Enabled

4.14 Remote Assistance

The remote assistance settings are discussed in the following section.

Computer Configuration > Administrative Templates> System > Remote Assistance

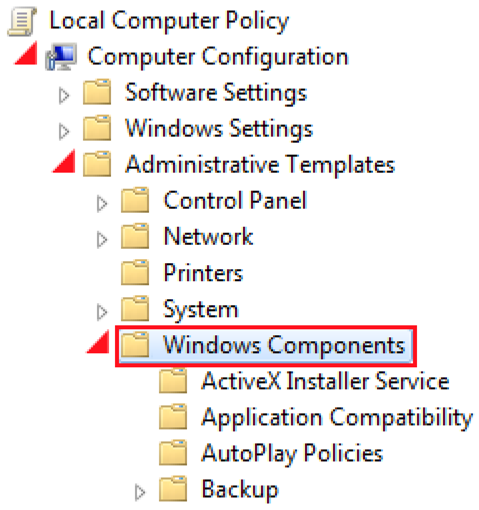
Setting	MUSA	P2P	Client/Server
Offer Remote Assistance	Disabled	Disabled	Disabled
Solicited Remote Assistance	Not Defined	Disabled	Disabled

4.15 Remote Procedure Call

Computer Configuration > Administrative Templates> System > Remote Procedure Call

Setting	Option Name	MUSA	P2P	Client/Server
Restrictions for Unauthenticated RPC clients		Not Defined	Enabled	Enabled
	RPC Runtime Unauthenticated Client Restriction to Apply		Authenticated	Authenticated
RPC Endpoint Mapper Client Authentication		Enabled	Enabled	Enabled

Group Policy | Computer Configuration > Administrative Templates > Windows Components



Local Computer Policy
Computer Configuration
Software Settings
Windows Settings
Administrative Templates
Control Panel
Network
Printers
System
Windows Components
ActiveX Installer Service
Application Compatibility
AutoPlay Policies
Backup

4.16 AutoPlay Policies

Computer Configuration > Administrative Templates > Windows Components > AutoPlay Policies

Setting	Option	MUSA, P2P, Client/Server
Turn off Autoplay		Enabled
Turn off Autoplay	Turn off Autoplay on	All drives
Default behavior for AutoRun		Enabled
	Default AutoRun Behavior	Do not execute any autorun commands
Turn off Autoplay for non-volume devices		Enabled

4.17 Credential User Interface

Computer Configuration > Administrative Templates > Windows Components > Credential User Interface

Setting	MUSA, P2P, Client/Server
Enumerate administrator accounts on elevation	Disabled
Require trusted path for credential entry.	Enabled

4.18 RSS Feeds

Computer Configuration > Administrative Templates > Windows Components > RSS Feeds

Setting	MUSA, P2P, Client/Server
Turn off downloading of enclosures	Enabled

4.19 HomeGroup

Computer Configuration > Administrative Templates > Windows Components > HomeGroup

Setting	MUSA, P2P, Client/Server
Prevent the computer from joining a homegroup	Enabled

4.20 Windows Explorer

Computer Configuration > Administrative Templates > Windows Components>Windows Explorer

Setting	MUSA, P2P, Client/Server
Turn off Data Execution Prevention for Explorer	Disabled

4.21 Windows Remote Shell

Computer Configuration > Administrative Templates > Windows Components > Windows Remote Shell

Setting	MUSA, P2P, Client/Server
Allow Remote Shell Access	Disabled

4.22 Windows Update

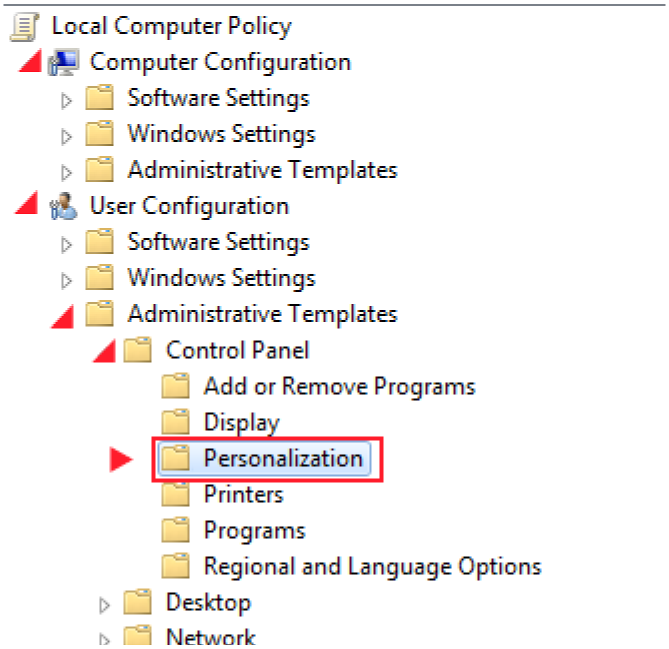
Computer Configuration > Administrative Templates > Windows Components > Windows Update

Setting	Option	MUSA, P2P, Client/Server
Configure Automatic Updates		Disabled
Do not adjust default option to 'Install Updates and Shut Down' in Shut Down Windows dialog box		Disabled
Do not display 'Install Updates and Shut Down' option in Shut Down Windows dialog box		Disabled
No auto-restart with logged on users for scheduled automatic updates installations		Disabled
Reschedule Automatic Updates scheduled installations		Enabled
	startup (minutes)	1 minute
Specify intranet Microsoft update service location		Not configured

5.0 User Level Group Policies

The following section references GP settings that must be made on the User, or Local GP.

5.1 Screen Saver Settings

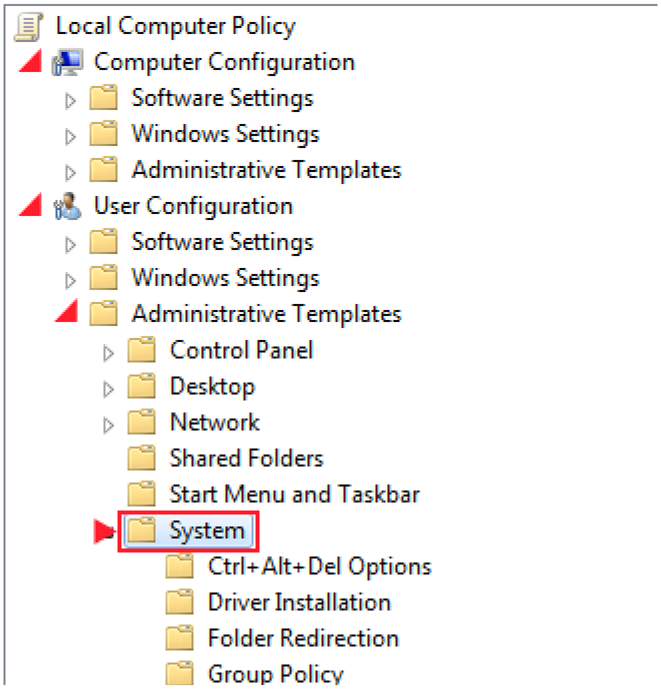


Local Computer Policy
- Computer Configuration
  - Software Settings
  - Windows Settings
  - Administrative Templates
- User Configuration
  - Software Settings
  - Windows Settings
  - Administrative Templates
    - Control Panel
      - Add or Remove Programs
      - Display
      - Personalization
      - Printers
      - Programs
      - Regional and Language Options
    - Desktop
    - Network

User Configuration>Administrative Templates>Control Panel>Personalization

Setting	Option	MUSA, P2P, Client/Server
Enable screen saver		Enabled
Force specific screen saver		Enabled
	Screen saver executable name	scrnsave.scr
Password protect the screen saver		Enabled
Screen saver timeout		Enabled
	Seconds	900

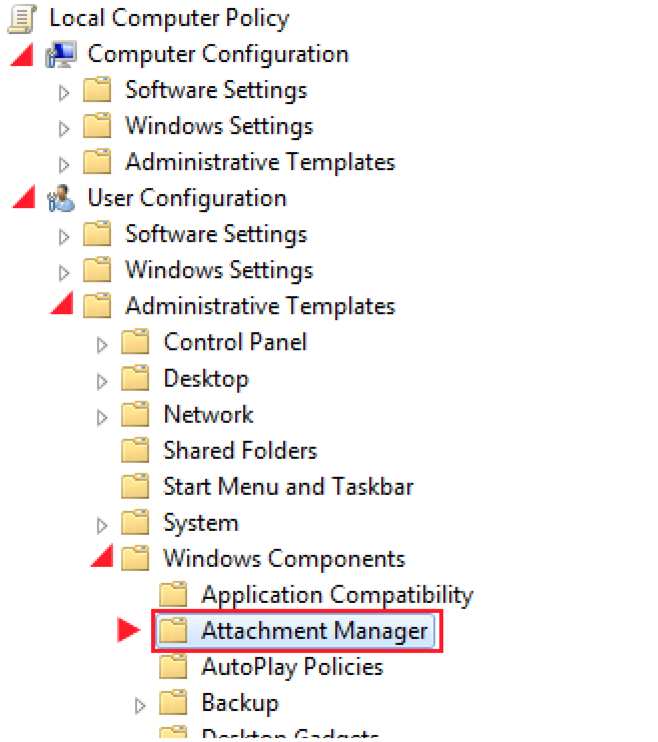
5.2 Registry Editing Options



User Configuration>Administrative Templates>System

Setting	Option	MUSA, P2P, Client/Server
Prevent access to registry editing tools		Enabled
	Disable regedit from running silently?	Yes

5.3 Attachment Manager



- Local Computer Policy
  - Computer Configuration
    - Software Settings
    - Windows Settings
    - Administrative Templates
  - User Configuration
    - Software Settings
    - Windows Settings
    - Administrative Templates
      - Control Panel
      - Desktop
      - Network
      - Shared Folders
      - Start Menu and Taskbar
      - System
      - Windows Components
        - Application Compatibility
        - Attachment Manager
        - AutoPlay Policies
        - Backup
        - Desktop Gadgets

Setting	MUSA, P2P, Client/Server
Do not preserve zone information in file attachments	Disabled
Hide mechanisms to remove zone information	Enabled
Notify antivirus programs when opening attachments	Enabled

5.4 Windows Explorer Settings

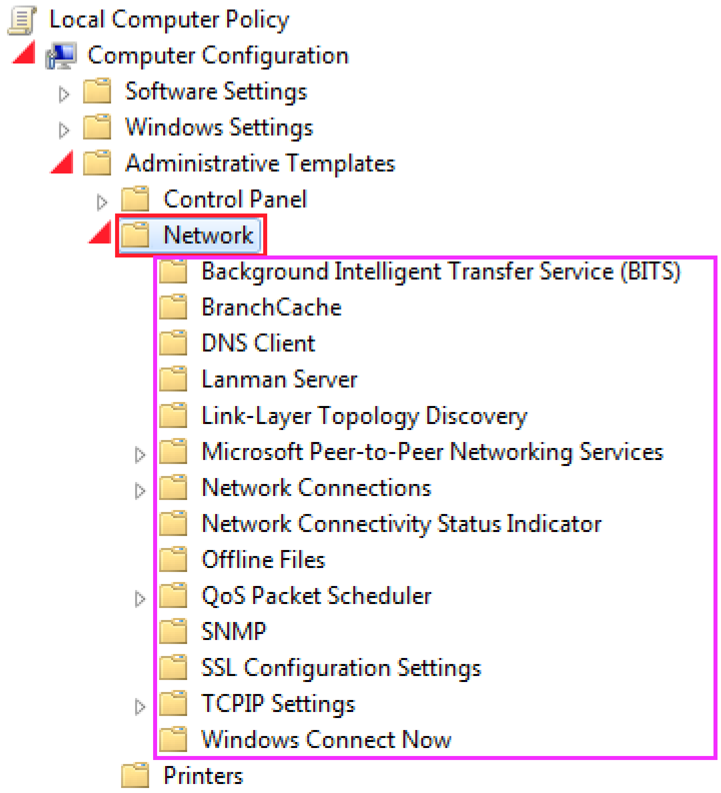
User Configuration>Administrative Templates>Windows Components>Windows Explorer

Setting	MUSA, P2P, Client/Server
Remove CD Burning features	Not Configured
Remove Security tab	Enabled

6.0 Additional GP Settings

The following section references additional GP settings.

6.1 Network Settings



- Local Computer Policy
  - Computer Configuration
    - Software Settings
    - Windows Settings
    - Administrative Templates
      - Control Panel
      - Network
        - Background Intelligent Transfer Service (BITS)
        - BranchCache
        - DNS Client
        - Lanman Server
        - Link-Layer Topology Discovery
        - Microsoft Peer-to-Peer Networking Services
        - Network Connections
        - Network Connectivity Status Indicator
        - Offline Files
        - QoS Packet Scheduler
        - SNMP
        - SSL Configuration Settings
        - TCPIP Settings
        - Windows Connect Now
      - Printers

The network settings are configured as follows.

Sub Folder	Setting	Option	MUSA	P2P	Client/Server
Link-Layer Topology Discovery	Turn on Mapper I/O (LLTDIO) driver		Disabled	Disabled	Disabled
Link-Layer Topology Discovery	Turn on Responder (RSPNDR) driver		Disabled	Disabled	Disabled
Microsoft Peer-to-Peer Networking Services	Turn off Microsoft Peer-to-Peer Networking Services		Enabled	Enabled	Enabled

Sub Folder	Setting	Option	MUSA	P2P	Client/Server
Network Connections	Prohibit installation and configuration of Network Bridge on your DNS domain network		Not Configured	Enabled	Enabled
Network Connections	Require domain users to elevate when setting a network's location		Not Configured	Not Configured	Enabled
Network Connections	Route all traffic through the internal network		Not Configured	Enabled	Enabled
		Select from the following states:			
TCPIP Settings\IPv6 Transition Technologies	6to4 State		Enabled	Enabled	Enabled
		Select from the following states:	Disabled State	Disabled State	Disabled State
TCPIP Settings\IPv6 Transition Technologies	IP-HTTPS State		Enabled	Enabled	Enabled
		Select Interface state from the following options:	Disabled State	Disabled State	Disabled State
TCPIP Settings\IPv6 Transition Technologies	ISATAP State		Enabled	Enabled	Enabled

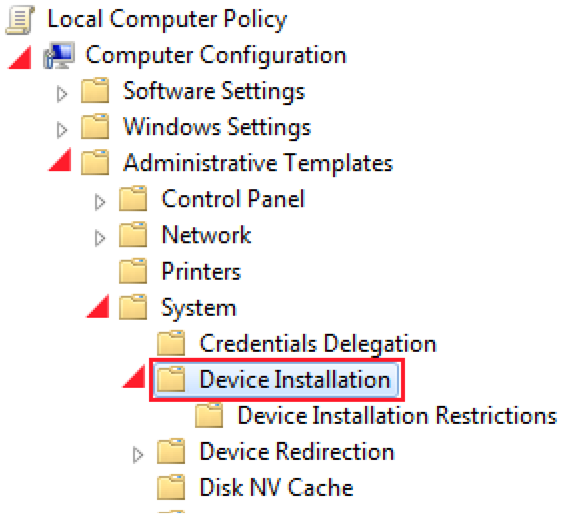
Sub Folder	Setting	Option	MUSA	P2P	Client/Server
		Select from the following states:	Disabled State	Disabled State	Disabled State
TCPIP Settings\IPv6 Transition Technologies	Teredo State		Enabled	Enabled	Enabled
		Select from the following states:	Disabled State	Disabled State	Disabled State
Windows Connect Now	Configuration of wireless settings using Windows Connect Now		Disabled	Disabled	Disabled
Windows Connect Now	Prohibit Access of the Windows Connect Now wizards		Enabled	Enabled	Enabled

6.2 Printers

Computer Configuration>Administrative Templates>Printers

Setting	MUSA, P2P, Client/Server
Extend Point and Print connection to search Windows Update	Disabled

6.3 Device Installation



Local Computer Policy
Computer Configuration
Software Settings
Windows Settings
Administrative Templates
Control Panel
Network
Printers
System
Credentials Delegation
Device Installation
Device Installation Restrictions
Device Redirection
Disk NV Cache

Computer Configuration>Administrative Templates>System>Device Installation

Setting	Option	MUSA, P2P, Client/Server
Allow remote access to the Plug and Play interface		Disabled
Do not send a Windows error report when a generic driver is installed on a device		Enabled
Prevent creation of a system restore point during device activity that would normally prompt creation of a restore point		Disabled
Prevent device metadata retrieval from the Internet		Enabled
Specify search order for device driver source locations		Enabled
	Select search order:	Do not search Windows Update

6.4 Driver Installation

Computer Configuration>Administrative Templates>System>Driver Installation

Setting	MUSA, P2P, Client/Server
Turn off Windows Update device driver search prompt	Enabled

6.5 Internet Communication

Computer Configuration>Administrative Templates>System>Internet Communication Management>Internet Communication settings

Setting	MUSA, P2P, Client/Server
Turn off Automatic Root Certificates Update	Enabled
Turn off downloading of print drivers over HTTP	Enabled
Turn off Event Viewer "Events.asp" links	Disabled
Turn off handwriting recognition error reporting	Enabled
Turn off Internet Connection Wizard if URL connection is referring to Microsoft.com	Enabled
Turn off Internet File Association service	Enabled
Turn off Registration if URL connection is referring to Microsoft.com	Enabled
Turn off the "Order Prints" picture task	Enabled
Turn off Windows Customer Experience Improvement Program	Enabled
Turn off Windows Error Reporting	Enabled
Turn off Windows Update device driver searching	Enabled
Handwriting Personalization Data Sharing	Enabled

6.6 Logon

Computer Configuration>Administrative Templates>System>Logon

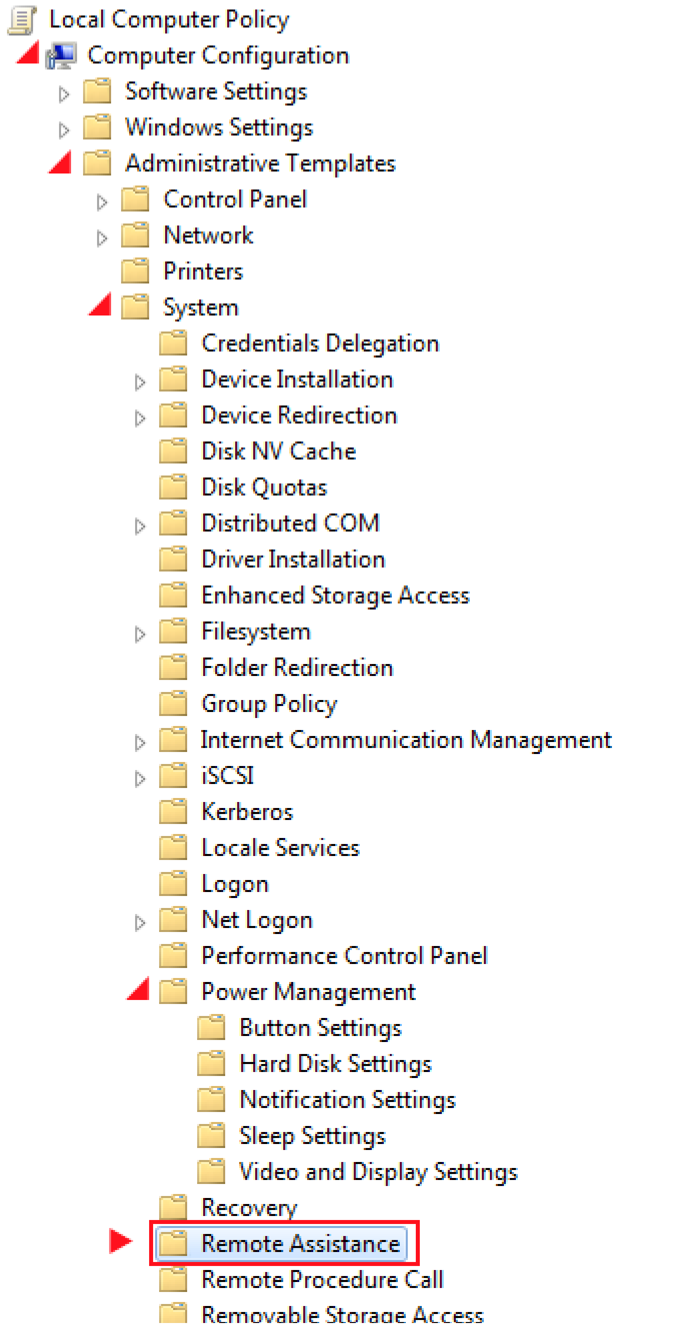
Setting	MUSA, P2P, Client/Server
Always use classic logon	Enabled

6.7 Sleep Settings

Computer Configuration>Administrative Templates>System>Power Management>Sleep Settings

Setting	MUSA, P2P, Client/Server
Require a Password When a Computer Wakes	Enabled

6.8 Remote Assistance



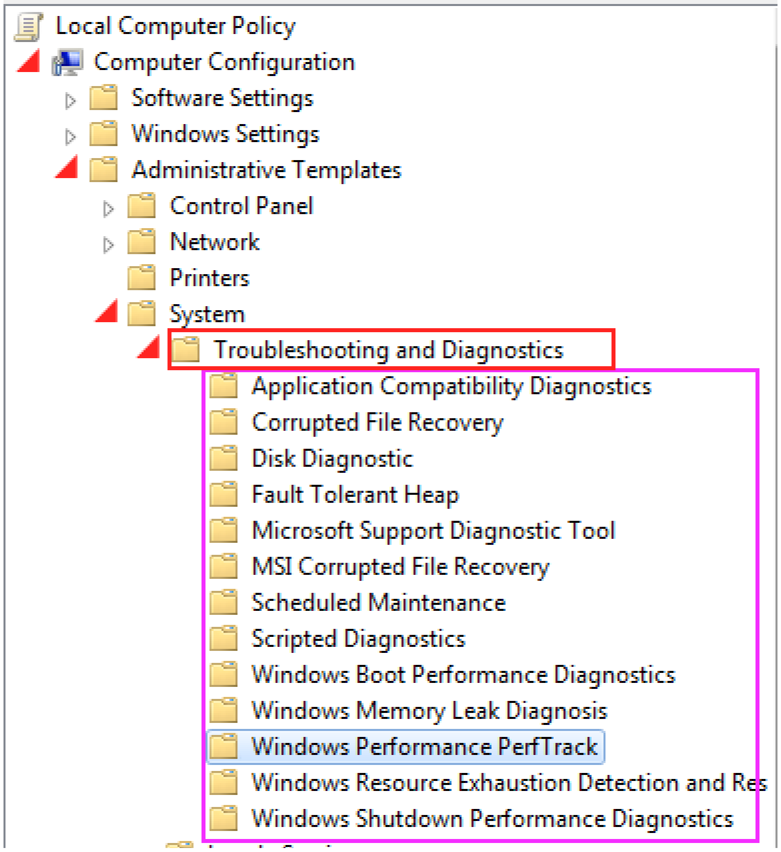
- Local Computer Policy
  - Computer Configuration
    - Software Settings
    - Windows Settings
    - Administrative Templates
      - Control Panel
      - Network
      - Printers
      - System
        - Credentials Delegation
        - Device Installation
        - Device Redirection
        - Disk NV Cache
        - Disk Quotas
        - Distributed COM
        - Driver Installation
        - Enhanced Storage Access
        - Filesystem
        - Folder Redirection
        - Group Policy
        - Internet Communication Management
        - iSCSI
        - Kerberos
        - Locale Services
        - Logon
        - Net Logon
        - Performance Control Panel
        - Power Management
          - Button Settings
          - Hard Disk Settings
          - Notification Settings
          - Sleep Settings
          - Video and Display Settings
        - Recovery
        - Remote Assistance
        - Remote Procedure Call
        - Removable Storage Access

The Remote Assistance settings are configured as demonstrated in the following table.

Computer Configuration>Administrative Templates>System>Remote Assistance

Setting	MUSA	P2P	Client/Server
Turn on session logging	Enabled	Enabled	Enabled
Solicited Remote Assistance	Not Configured	Disabled	Disabled
Offer Remote Assistance	Not Configured	Disabled	Disabled

6.9 Troubleshooting and Diagnostics



- Local Computer Policy
  - Computer Configuration
    - Software Settings
    - Windows Settings
    - Administrative Templates
      - Control Panel
      - Network
      - Printers
      - System
        - Troubleshooting and Diagnostics
          - Application Compatibility Diagnostics
          - Corrupted File Recovery
          - Disk Diagnostic
          - Fault Tolerant Heap
          - Microsoft Support Diagnostic Tool
          - MSI Corrupted File Recovery
          - Scheduled Maintenance
          - Scripted Diagnostics
          - Windows Boot Performance Diagnostics
          - Windows Memory Leak Diagnosis
          - Windows Performance PerfTrack
          - Windows Resource Exhaustion Detection and Res
          - Windows Shutdown Performance Diagnostics

Sub Folder	Setting	MUSA, P2P, Client/Server
Microsoft Support Diagnostic Tool	Turn on MSDT interactive communication with Support Provider	Disabled
Windows Performance PerfTrack	Enable/Disable PerfTrack	Disabled
Scripted Diagnostics	Troubleshooting: Allow users to access online troubleshooting content on Microsoft servers from the Troubleshooting Control Panel (via the Windows Online Troubleshooting Service - WOTS)	Disabled

6.10 Windows Time Service

Computer Configuration>Administrative Templates>System\Windows Time Service>Time Providers

Setting	Option	MUSA, P2P, Client/Server
Configure Windows NTP Client		Enabled

	CrossSiteSyncFlags	2
	EventLogFlags	0
	NtpServer	localtimeserver
	ResolvePeerBackoffMaxTimes	7
	ResolvePeerBackoffMinutes	15
	SpecialPollInterval	3600
	Type	NT5D5

6.11 Application Compatibility

The Application Compatibility settings are configured as follows.

Computer Configuration>Administrative Templates>Windows Components>Application Compatibility

Setting	MUSA, P2P, Client/Server
Turn off Program Inventory	Enabled

6.12 Desktop Gadgets

The desktop gadgets settings are configured as follows.

Computer Configuration>Administrative Templates>Windows Components>Desktop Gadgets

Setting	MUSA, P2P, Client/Server
Override the More Gadgets link	Enabled with "about:blank" entered in the option
Turn Off user-installed desktop gadgets	Enabled
Restrict unpacking and installation of gadgets that are not digitally signed.	Enabled

6.13 Event Log Service

The Event Log Service settings are configured as demonstrated below.

Computer Configuration>Administrative Templates>Windows Components>Event Log Service

Category	Setting	Option	MUSA, P2P, Client/Server

Category	Setting	Option	MUSA, P2P, Client/Server
Application	Maximum Log Size (KB)		Enabled
		Maximum Log Size (KB)	81920*
Security	Maximum Log Size (KB)		Enabled
		Maximum Log Size (KB)	81920*
Setup	Maximum Log Size (KB)		Enabled
		Maximum Log Size (KB)	32768*

*Note: The log sizes shown here are an example of best practice throughout industry. Due to operational environment, this figure is subject to change.

6.14 Game Explorer

The game explorer settings are configured as demonstrated below.

Computer Configuration>Administrative Templates>Windows Components>Game Explorer

Setting	MUSA, P2P, Client/Server
Turn off downloading of game information	Enabled
Turn off game updates	Enabled

6.15 HomeGroup

Configure the HomeGroup settings as shown in the table below.

Computer Configuration>Administrative Templates>Windows Components>HomeGroup

Setting	MUSA, P2P, Client/Server
Prevent the computer from joining a homegroup	Enabled

6.16 Remote Desktop Services

The Remote Desktop Services settings are configured as shown below.
Computer Configuration>Administrative Templates>Windows Components>Remote Desktop Services>

Subfolder	Setting	Option	MUSA	P2P	Client/Server
Remote Desktop Connection Client	Do not allow passwords to be saved		Enabled	Enabled	Enabled
Remote Desktop Session Host\Connections	Allow users to connect remotely using Remote Desktop Services		Disabled	Disabled	Disabled
Remote Desktop Session Host\Device and Resource Redirection	Do not allow drive redirection		Enabled	Enabled	Enabled
Remote Desktop Session Host\Security	Always prompt for password upon connection		Enabled	Enabled	Enabled
Remote Desktop Session Host\Security	Set client connection encryption level		Enabled	Enabled	Enabled
		Encryption Level	High Level	High Level	High Level
Remote Desktop Session Host\Session Time Limits	Set time limit for active but idle Remote Desktop Services sessions		Enabled	Enabled	Enabled
		Idle session limit:	15 minutes	15 minutes	15 minutes
Remote Desktop Session Host\Session Time Limits	Set time limit for disconnected sessions		Enabled	Enabled	Enabled
		End a disconnected session	1 minute	1 minute	1 minute

Subfolder	Setting	Option	MUSA	P2P	Client/Server
Remote Desktop Session Host\Temporary folders	Do not delete temp folder upon exit		Disabled	Disabled	Disabled
Remote Desktop Session Host \ Connections	Do not use temporary folders per session		Disabled	Disabled	Disabled
	Restrict Remote Desktop Services users to a Single Remote Desktop Services Session		Not defined	Not defined	Enabled
Remote Desktop Session Host \ Device and Resource Redirection	Do not allow clipboard redirection		Not defined	Not defined	Enabled
Remote Desktop Session Host \ Device and Resource Redirection	Do not allow COM port redirection		Not defined	Not defined	Enabled
Remote Desktop Session Host \ Device and Resource Redirection	Do not allow LPT port redirection		Not defined	Not defined	Enabled
Remote Desktop Session Host \ Device and Resource Redirection	Do not allow supported Plug and Play device redirection		Not defined	Not defined	Enabled
Remote Desktop Session Host \ Device and Resource Redirection	Do not allow smart card device redirection		Not defined	Not defined	Not defined

Subfolder	Setting	Option	MUSA	P2P	Client/Server
Remote Desktop Session Host \ Printer Redirection	Redirect only the default client printer		Not defined	Not defined	Enabled
Remote Desktop Session Host \ Remote Session Environment	Remove Disconnect option from Shut Down dialog		Not defined	Not defined	Enabled

6.17 Windows Anytime Upgrade

The Windows Anytime Upgrade settings are configured as shown below.

Computer Configuration>Administrative Templates>Windows Components>Windows Anytime Upgrade

Setting	MUSA, P2P, Client/Server
Prevent Windows Anytime Upgrade from running.	Enabled

6.18 Windows Defender

The Windows Defender settings are configured as demonstrated in the following table.

Computer Configuration>Administrative Templates>Windows Components>Windows Defender

Setting	MUSA, P2P, Client/Server
Configure Microsoft SpyNet Reporting	Disabled

6.19 Windows Error Reporting

The Windows Error Reporting settings are configured as follows.

Computer Configuration>Administrative Templates>Windows Components>Windows Error Reporting

Setting	UI Path	MUSA, P2P, Client/Server
Disable Logging		Disabled
Disable Windows Error Reporting		Enabled

Do not send additional data		Enabled

6.20 Windows Explorer

Computer Configuration>Administrative Templates>Windows Components>Windows Explorer

Setting	MUSA, P2P, Client/Server
Turn off Data Execution Prevention for Explorer	Disabled
Turn off heap termination on corruption	Disabled
Turn off shell protocol protected mode	Disabled

6.21 Windows Installer

Computer Configuration\Administrative Templates>Windows Components>Windows Installer

Setting	MUSA, P2P, Client/Server
Disable IE security prompt for Windows Installer scripts	Disabled
Enable user control over installs	Disabled
Prohibit non-administrators from applying vendor signed updates	Enabled
Always install with elevated privileges	Disabled

6.22 Windows Logon Options

The Windows Logon Options settings are configured as shown in the table below.

Computer Configuration>Administrative Templates>Windows Components>Windows Logon Options

Setting	MUSA, P2P, Client/Server
Report when logon server was not available during user logon	Enabled

6.23 Windows Media Digital Rights Management

The Windows Media Digital Rights Management settings are configured as shown in the following table.

Computer Configuration>Administrative Templates>Windows Components>Windows Media Digital Rights Management

Setting	MUSA, P2P, Client/Server
Prevent Windows Media DRM Internet Access	Enabled

6.24 Windows Media Play

The Windows Media Player settings are configured as shown below.

Computer Configuration>Administrative Templates>Windows Components>Windows Media Player

Setting	MUSA, P2P, Client/Server
Do Not Show First Use Dialog Boxes	Enabled
Prevent Automatic Updates	Enabled

6.25 Windows Search Settings

Computer Configuration >Administrative Templates >Windows Components >Search

Setting	MUSA, P2P, Client/Server
Search – Encrypted Files Indexing	Disabled
Search – Exchange Folder Indexing	Disabled

7.0 File Permissions for Security Relevant Objects

NISPOM chapter 8 requires file permissions to be set for security relevant objects as described in the following tables. Note that not all of these security relevant objects exist in all versions of Windows 7 and Windows Server 2008. Also, it is implicit that auditing of Fail access to these objects will be configured as described in section 7.1.

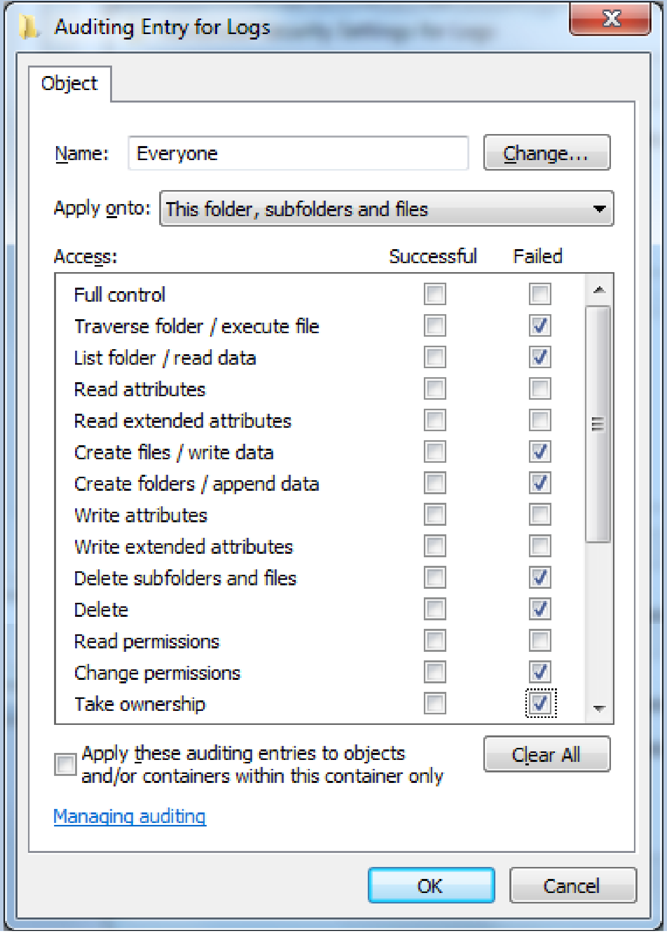
7.1 File Auditing for Security Relevant Objects

Windows 7 and Windows 2008 Server provide a method to monitor access to any file or folder 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 and folder auditing, perform the following steps:

1. Right-click on the file/folder, 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. Configurations:

For PL 1 systems configure the following file permission access attributes:

Folder Auditing Attributes



Auditing Entry for Logs

Object

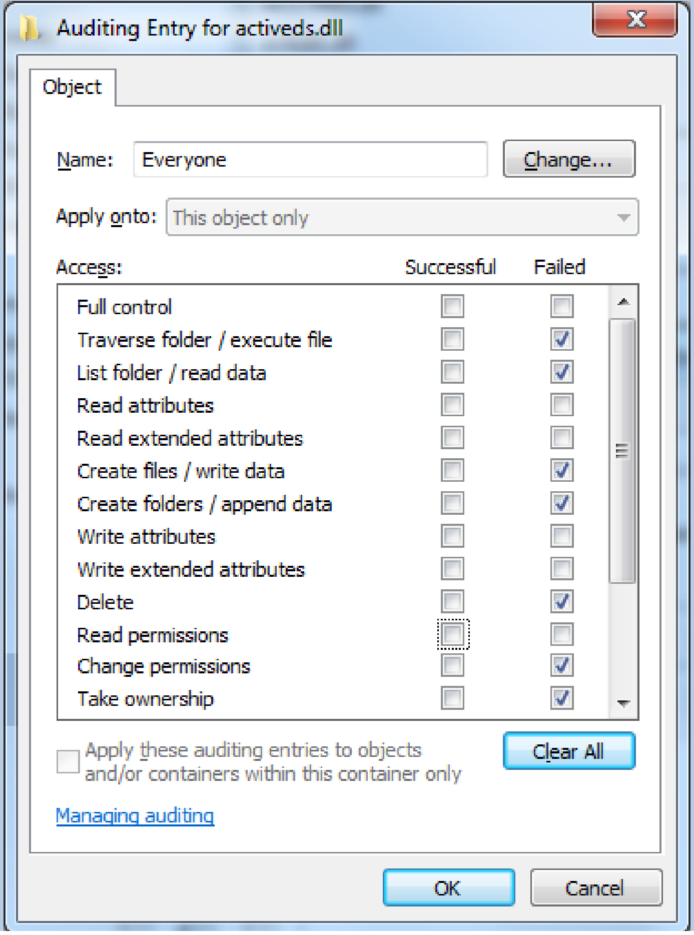
Name: Everyone

Apply onto: This folder, subfolders and files

Access:	Successful	Failed
Full control	☐	☐
Traverse folder / execute file	☐	☑
List folder / read data	☐	☑
Read attributes	☐	☐
Read extended attributes	☐	☐
Create files / write data	☐	☑
Create folders / append data	☐	☑
Write attributes	☐	☐
Write extended attributes	☐	☐
Delete subfolders and files	☐	☑
Delete	☐	☑
Read permissions	☐	☐
Change permissions	☐	☑
Take ownership	☐	☑

☐ Apply these auditing entries to objects and/or containers within this container only

File Auditing Attributes



Auditing Entry for activeds.dll

Object

Name: Everyone

Apply onto: This object only

Access:	Successful	Failed
Full control	☐	☐
Traverse folder / execute file	☐	☑
List folder / read data	☐	☑
Read attributes	☐	☐
Read extended attributes	☐	☐
Create files / write data	☐	☑
Create folders / append data	☐	☑
Write attributes	☐	☐
Write extended attributes	☐	☐
Delete	☐	☑
Read permissions	☐	☐
Change permissions	☐	☑
Take ownership	☐	☑

☐ Apply these auditing entries to objects and/or containers within this container only

For PL 2 systems configure the following file permission access attributes: Select Full Control Failed check box to capture all failed check boxes.

File SROs for Windows 7

\%Windows%\System32\winevt\Logs
\%Windows%\System32\config
\%Windows%\System32\activeds.dll
\%Windows%\System32\adsldpc.dll
\%Windows%\System32\advapi32.dll
\%Windows%\System32\advpack.dll
\%Windows%\System32\apphelp.dll
\%Windows%\System32\arp.exe
\%Windows%\System32\at.exe
\%Windows%\System32\atl.dll
\%Windows%\System32\attrib.exe
\%Windows%\System32\authz.dll
\%Windows%\System32\bootvid.dll
\%Windows%\System32\browseui.dll
\%Windows%\System32\cabinet.dll
\%Windows%\System32\cacls.exe
\%Windows%\System32\certcli.dll
\%Windows%\System32\cfgmgr32.dll
\%Windows%\System32\clbcatq.dll
\%Windows%\System32\clusapi.dll
\%Windows%\System32\comdlg32.dll
\%Windows%\System32\comres.dll
\%Windows%\System32\config
\%Windows%\System32\credui.dll
\%Windows%\System32\crypt32.dll
\%Windows%\System32\cryptdll.dll
\%Windows%\System32\cryptui.dll
\%Windows%\System32\cscdll.dll
\%Windows%\System32\dbghelp.dll
\%Windows%\System32\devmgr.dll
\%Windows%\System32\dhcpcsvc.dll
\%Windows%\System32\dnsapi.dll
\%Windows%\System32\drivers\ksecdd.sys
\%Windows%\System32\DRIVERS\ntfs.sys
\%Windows%\System32\duser.dll
\%Windows%\System32\efsadu.dll
\%Windows%\System32\esent.dll
\%Windows%\System32\eventcreate.exe
\%Windows%\System32\ftp.exe
\%Windows%\System32\gdi32.dll
\%Windows%\System32\hal.dll
\%Windows%\System32\imagehlp.dll
\%Windows%\System32\imm32.dll
\%Windows%\System32\inetcomm.dll
\%Windows%\System32\iphlpapi.dll
\%Windows%\System32\kdcom.dll
\%Windows%\System32\kdcsvc.dll
\%Windows%\System32\kerberos.dll
\%Windows%\System32\kernel32.dll
\%Windows%\System32\linkinfo.dll
\%Windows%\System32\loadperf.dll
\%Windows%\System32\lsasrv.dll
\%Windows%\System32\lsass.exe
\%Windows%\System32\lz32.dll
\%Windows%\System32\mfc42u.dll
\%Windows%\System32\mlang.dll
\%Windows%\System32\mobsync.exe
\%Windows%\System32\mpr.dll
\%Windows%\System32\mprapi.dll
\%Windows%\System32\msasn1.dll
\%Windows%\System32\msgina.dll
\%Windows%\System32\mshtml.dll
\%Windows%\System32\msi.dll
\%Windows%\System32\msimg32.dll
\%Windows%\System32\msoert2.dll
\%Windows%\System32\msrating.dll
\%Windows%\System32\mssign32.dll
\%Windows%\System32\msv1_0.dll
\%Windows%\System32\msvcp60.dll
\%Windows%\System32\msvcrt.dll
\%Windows%\System32\mswsock.dll
\%Windows%\System32\nbtstat.exe
\%Windows%\System32\nddeapi.dll
\%Windows%\System32\net.exe
\%Windows%\System32\net1.exe
\%Windows%\System32\netapi32.dll
\%Windows%\System32\netcfgx.dll
\%Windows%\System32\netman.dll
\%Windows%\System32\netplwiz.dll
\%Windows%\System32\netsh.exe
\%Windows%\System32\netshell.dll
\%Windows%\System32\netstat.exe
\%Windows%\System32\ntbackup.exe
\%Windows%\System32\ntdll.dll

\%Windows%\System32\ntdsa.dll
\%Windows%\System32\ntdsapi.dll
\%Windows%\System32\ntdsatq.dll
\%Windows%\System32\ntlanman.dll
\%Windows%\System32\ntoskrnl.exe
\%Windows%\System32\odbc32.dll
\%Windows%\System32\ole32.dll
\%Windows%\System32\oleacc.dll
\%Windows%\System32\oleaut32.dll
\%Windows%\System32\oledlg.dll
\%Windows%\System32\pautoenr.dll
\%Windows%\System32\powrprof.dll
\%Windows%\System32\printui.dll
\%Windows%\System32\psapi.dll
\%Windows%\System32\query.dll
\%Windows%\System32\rasapi32.dll
\%Windows%\System32\rasdlg.dll
\%Windows%\System32\rasman.dll
\%Windows%\System32\reg.exe
\%Windows%\System32\regapi.dll
\%Windows%\System32\regedt32.exe
\%Windows%\System32\regini.exe
\%Windows%\System32\regsvr32.exe
\%Windows%\System32\route.exe
\%Windows%\System32\rpcrt4.dll
\%Windows%\System32\rshx32.exe
\%Windows%\System32\rtutils.dll
\%Windows%\System32\samlib.dll
\%Windows%\System32\samsrv.dll
\%Windows%\System32\sc.exe
\%Windows%\System32\scecli.dll
\%Windows%\System32\secedit.exe
\%Windows%\System32\secur32.dll
\%Windows%\System32\security.dll
\%Windows%\System32\setupapi.dll
\%Windows%\System32\sfc.dll
\%Windows%\System32\shdocvw.dll
\%Windows%\System32\shlwapi.dll
\%Windows%\System32\shsvcs.dll
\%Windows%\System32\subst.exe
\%Windows%\System32\systeminfo.exe
\%Windows%\System32\tapi32.dll
\%Windows%\System32\urlmon.dll
\%Windows%\System32\user32.dll
\%Windows%\System32\userenv.dll
\%Windows%\System32\utildll.dll
\%Windows%\System32\uxtheme.dll
\%Windows%\System32\version.dll
\%Windows%\System32\w32topl.dll
\%Windows%\System32\wininet.dll
\%Windows%\System32\winipsec.dll
\%Windows%\System32\winlogon.exe
\%Windows%\System32\winmm.dll
\%Windows%\System32\winscard.dll
\%Windows%\System32\winspool.drv
\%Windows%\System32\winsta.dll
\%Windows%\System32\wintrust.dll
\%Windows%\System32\wldap32.dll
\%Windows%\System32\wmi.dll
\%Windows%\System32\ws2_32.dll
\%Windows%\System32\ws2help.dll
\%Windows%\System32\wsock32.dll
\%Windows%\System32\wtsapi32.dll
\%Windows%\System32\wzcdlg.dll
\%Windows%\System32\regedit.exe
\%Windows%\System32\timedate.cpl

\%Windows%\winsxs\x86_microsoft-Windows-msvbvm60_31bf3856ad364e35_6.1.7600.16385_none_c25a1af6b30d72ee\msvbvm60.dll

\%Windows%\winsxs\amd64_microsoft-Windows-telnet-client_31bf3856ad364e35_6.1.7600.16385_none_1426830c3ebb712d\telnet.exe

\%Windows%\winsxs\amd64_microsoft-Windows-t..-deployment-package_31bf3856ad364e35_6.1.7600.16385_none_bac291589d407fde\tftp.exe

\%Windows%\winsxs\amd64_microsoft-Windows-telnet-server-tlntsvr_31bf3856ad364e35_6.1.7600.16385_none_1ab997fb0a83afdd\tlntsvr.exe

File SROs for Windows 7 64bit Machines

\%Windows%\SysWOW64\activeds.dll
\%Windows%\SysWOW64\adsldpc.dll

\%Windows%\SysWOW64\advapi32.dll
\%Windows%\SysWOW64\advpack.dll
\%Windows%\SysWOW64\arp.exe
\%Windows%\SysWOW64\at.exe
\%Windows%\SysWOW64\atl.dll
\%Windows%\SysWOW64\attrib.exe
\%Windows%\SysWOW64\apphelp.dll
\%Windows%\SysWOW64\authz.dll
\%Windows%\SysWOW64\bootvid.dll
\%Windows%\SysWOW64\browseui.dll
\%Windows%\SysWOW64\cabinet.dll
\%Windows%\SysWOW64\cacls.exe
\%Windows%\SysWOW64\certcli.dll
\%Windows%\SysWOW64\cfgmgr32.dll
\%Windows%\SysWOW64\clbcatq.dll
\%Windows%\SysWOW64\clusapi.dll
\%Windows%\SysWOW64\comdlg32.dll
\%Windows%\SysWOW64\comres.dll
\%Windows%\SysWOW64\credui.dll
\%Windows%\SysWOW64\crypt32.dll
\%Windows%\SysWOW64\cryptdll.dll
\%Windows%\SysWOW64\cryptui.dll
\%Windows%\SysWOW64\cscdll.dll
\%Windows%\SysWOW64\dbghelp.dll
\%Windows%\SysWOW64\devmgr.dll
\%Windows%\SysWOW64\dhcpcsvc.dll
\%Windows%\SysWOW64\dnsapi.dll
\%Windows%\SysWOW64\duser.dll
\%Windows%\SysWOW64\efsadu.dll
\%Windows%\SysWOW64\esent.dll
\%Windows%\SysWOW64\eventcreate.exe
\%Windows%\SysWOW64\ftp.exe
\%Windows%\SysWOW64\gdi32.dll
\%Windows%\SysWOW64\imagehlp.dll
\%Windows%\SysWOW64\imm32.dll
\%Windows%\SysWOW64\inetcomm.dll
\%Windows%\SysWOW64\iphlpapi.dll
\%Windows%\SysWOW64\kerberos.dll
\%Windows%\SysWOW64\kernel32.dll
\%Windows%\SysWOW64\linkinfo.dll
\%Windows%\SysWOW64\loadperf.dll
\%Windows%\SysWOW64\lz32.dll
\%Windows%\SysWOW64\mfc42u.dll
\%Windows%\SysWOW64\mlang.dll
\%Windows%\SysWOW64\mobsync.exe
\%Windows%\SysWOW64\mpr.dll
\%Windows%\SysWOW64\mprapi.dll
\%Windows%\SysWOW64\msasn1.dll
\%Windows%\SysWOW64\mshtml.dll
\%Windows%\SysWOW64\msi.dll
\%Windows%\SysWOW64\msimg32.dll
\%Windows%\SysWOW64\msoert2.dll
\%Windows%\SysWOW64\msrating.dll
\%Windows%\SysWOW64\mssign32.dll
\%Windows%\SysWOW64\msv1_0.dll
\%Windows%\SysWOW64\msvcp60.dll
\%Windows%\SysWOW64\msvcrt.dll
\%Windows%\SysWOW64\mswsock.dll
\%Windows%\SysWOW64\nddeapi.dll
\%Windows%\SysWOW64\net.exe
\%Windows%\SysWOW64\net1.exe
\%Windows%\SysWOW64\netapi32.dll
\%Windows%\SysWOW64\netcfgx.dll
\%Windows%\SysWOW64\netplwiz.dll
\%Windows%\SysWOW64\netsh.exe
\%Windows%\SysWOW64\netshell.dll
\%Windows%\SysWOW64\netstat.exe
\%Windows%\SysWOW64\nslookup.exe
\%Windows%\SysWOW64\ntdll.dll
\%Windows%\SysWOW64\ntdsapi.dll
\%Windows%\SysWOW64\ntlanman.dll
\%Windows%\SysWOW64\ntoskrnl.exe
\%Windows%\SysWOW64\odbc32.dll
\%Windows%\SysWOW64\ole32.dll
\%Windows%\SysWOW64\oleacc.dll
\%Windows%\SysWOW64\oleaut32.dll
\%Windows%\SysWOW64\oledlg.dll
\%Windows%\SysWOW64\olepro32.dll
\%Windows%\SysWOW64\pautoenr.dll
\%Windows%\SysWOW64\powrprof.dll
\%Windows%\SysWOW64\printui.dll
\%Windows%\SysWOW64\psapi.dll
\%Windows%\SysWOW64\query.dll
\%Windows%\SysWOW64\rasapi32.dll
\%Windows%\SysWOW64\rasdlg.dll
\%Windows%\SysWOW64\rasman.dll
\%Windows%\SysWOW64\reg.exe
\%Windows%\SysWOW64\regapi.dll
\%Windows%\SysWOW64\regedt32.exe
\%Windows%\SysWOW64\regini.exe
\%Windows%\SysWOW64\regsvr32.exe
\%Windows%\SysWOW64\route.exe
\%Windows%\SysWOW64\rpcrt4.dll
\%Windows%\SysWOW64\rshx32.exe
\%Windows%\SysWOW64\rtutils.dll
\%Windows%\SysWOW64\samlib.dll
\%Windows%\SysWOW64\sc.exe
\%Windows%\SysWOW64\scecli.dll

\%Windows%\SysWOW64\secedit.exe
\%Windows%\SysWOW64\secur32.dll
\%Windows%\SysWOW64\security.dll
\%Windows%\SysWOW64\setupapi.dll
\%Windows%\SysWOW64\sfc.dll
\%Windows%\SysWOW64\shdocvw.dll
\%Windows%\SysWOW64\shlwapi.dll
\%Windows%\SysWOW64\shsvcs.dll
\%Windows%\SysWOW64\subst.exe
\%Windows%\SysWOW64\systeminfo.exe
\%Windows%\SysWOW64\tapi32.dll
\%Windows%\SysWOW64\urlmon.dll
\%Windows%\SysWOW64\user32.dll
\%Windows%\SysWOW64\userenv.dll
\%Windows%\SysWOW64\utildll.dll
\%Windows%\SysWOW64\uxtheme.dll
\%Windows%\SysWOW64\version.dll
\%Windows%\SysWOW64\w32topl.dll
\%Windows%\SysWOW64\wininet.dll
\%Windows%\SysWOW64\winipsec.dll
\%Windows%\SysWOW64\winmm.dll
\%Windows%\SysWOW64\winscard.dll
\%Windows%\SysWOW64\winspool.drv
\%Windows%\SysWOW64\winsta.dll
\%Windows%\SysWOW64\wintrust.dll
\%Windows%\SysWOW64\wldap32.dll
\%Windows%\SysWOW64\wmi.dll
\%Windows%\SysWOW64\ws2_32.dll
\%Windows%\SysWOW64\ws2help.dll
\%Windows%\SysWOW64\wsock32.dll
\%Windows%\SysWOW64\wtsapi32.dll
\%Windows%\SysWOW64\wzcdlg.dll
\%Windows%\SysWOW64\regedit.exe
\%Windows%\SysWOW64\spool\printers

8.0 Additional Requirements

8.1 Disallow AutoPlay/Autorun

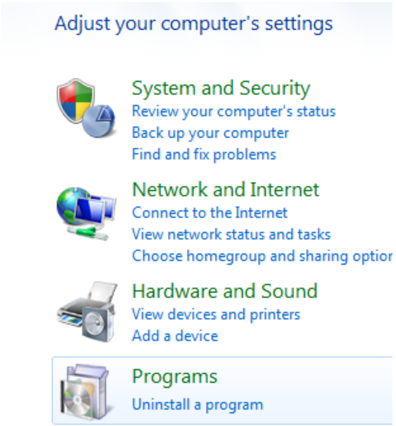
Setting Name	Setting	MUSA P2P Client/ Server
Disallow AutoPlay/Autorun from Autorun.inf	Disable AutoRun in Microsoft Windows To effectively disable AutoRun in Microsoft Windows, import the following registry value: **REGEDIT4** **[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\IniFileMapping\Autorun.inf]** **@="@SYS:DoesNotExist"** To import this value, perform the following steps: 1. Copy the text 2. Paste the text into Windows Notepad 3. Save the file as "autorun.reg" Note: In certain circumstances, Notepad may automatically add a .txt extension to saved files. To ensure that the file is saved with the proper extension, select All Files in the "Save as type:" section of the "Save As" dialog. 4. Navigate to the file location 5. Double-click the file to import it into the Windows registry Microsoft Windows can also cache the AutoRun information from mounted devices in the MountPoints2 registry key. We recommend restarting Windows after making the registry change so that any cached mount points are reinitialized in a way that ignores the Autorun.inf file. Alternatively, the following registry key may be deleted: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2	Add new registry value

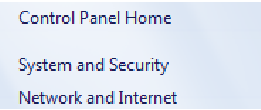
8.2 Programs and Features

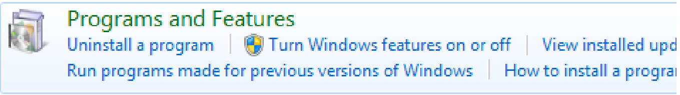
Microsoft Windows operating systems include additional features that are unnecessary and can create vulnerabilities. The following features shall be uninstalled or turned off.

To turn off these features go to Control Panel > Select Category (Top Right) > Click Programs > Turn Windows Features on or off

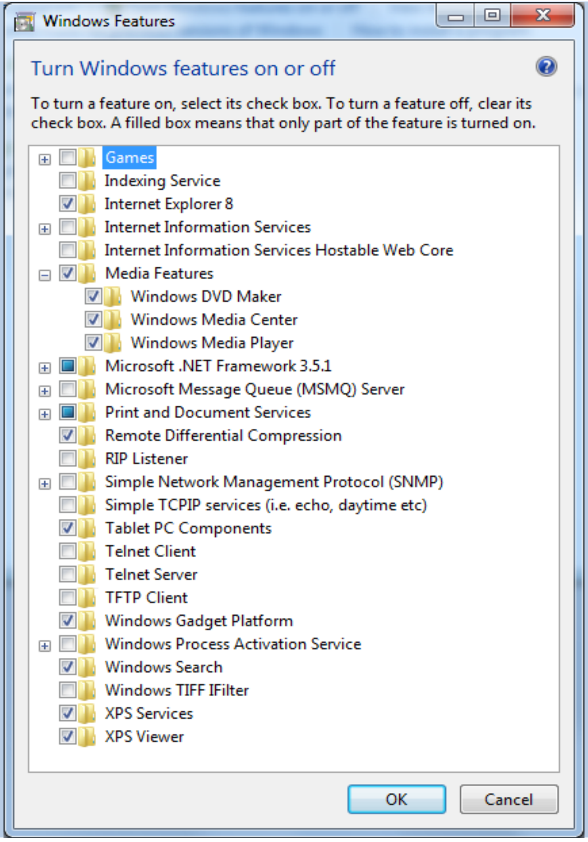
1 2






Programs and Features
Uninstall a program
Turn Windows features on or off
View installed upd
Run programs made for previous versions of Windows
How to install a progra

Uncheck the items you want to turn off:

Setting	MUSA, P2P, Client/Server	
Games Internet Information Services Windows Media Center (under Media Features) SimpleTCPIP Services Telnet (Client or Server) TFTP Client	Off (Uncheck)	 Windows Features Turn Windows features on or off To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on. □ Games □ Indexing Service ☑ Internet Explorer 8 □ Internet Information Services □ Internet Information Services Hostable Web Core ☑ Media Features ☑ Windows DVD Maker ☑ Windows Media Center ☑ Windows Media Player ■ Microsoft .NET Framework 3.5.1 □ Microsoft Message Queue (MSMQ) Server ■ Print and Document Services ☑ Remote Differential Compression □ RIP Listener □ Simple Network Management Protocol (SNMP) □ Simple TCPIP services (i.e. echo, daytime etc) ☑ Tablet PC Components □ Telnet Client □ Telnet Server □ TFTP Client ☑ Windows Gadget Platform □ Windows Process Activation Service ☑ Windows Search □ Windows TIFF IFilter ☑ XPS Services ☑ XPS Viewer OK Cancel

8.3 Services

Windows 7 and Windows Server 2008 R2 automatically start numerous services some of which are not required and often pose security threats. Any services not required shall be disabled.

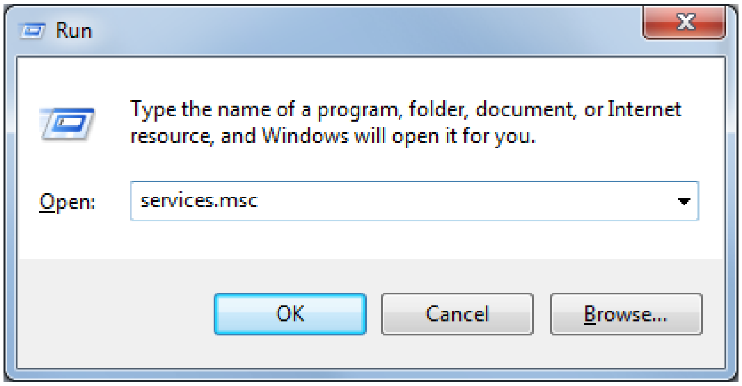
The following services will be disabled.

Setting	MUSA, P2P, Client/Server
Fax Remote Access Auto Connection Manager Remote Access Connection Manager Remote Desktop Help Session Manager Routing and Remote Access SNMP Service SNMP Trap Service Simple Service Discovery Protocol Discovery Service Telnet Universal Plug and Play Device Host Windows Firewall/Internet Connection Sharing Windows Update WLAN AutoConfig World Wide Web Publishing Services	Disabled

To disable services:

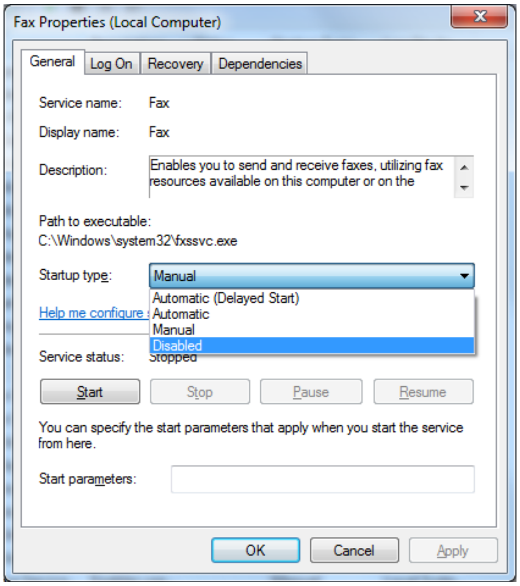
Start > Run (or Windows Key + R) type services.msc:

Double click the above services and select disable from the dropdown:



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: services.msc



Service name: Fax

Display name: Fax

Description: Enables you to send and receive faxes, utilizing fax resources available on this computer or on the

Path to executable:
C:\Windows\system32\fxssvc.exe

Startup type: Manual

Service status: Stopped

You can specify the start parameters that apply when you start the service from here.

Start parameters:

9.0 Vulnerabilities

9.1 Account Policies

Paragraph	Vulnerability
4.2.1	The longer a user uses the same password, the greater the chance that an attacker can 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 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 might repeatedly change their passwords until they can reuse their original password.
4.2.2	The longer a password exists the higher the likelihood that it will be compromised by a brute force attack, by an attacker gaining general knowledge about the user, or by the user sharing the password. Configuring the Maximum password age setting to 0 so that users are never required to change their passwords is a major security risk because that allows a compromised password to be used by the malicious user for as long as the valid user is authorized access.

4.2.3	Users may have favorite passwords that they like to use because they are easy to remember and they believe that their password choice is secure from compromise. Unfortunately, passwords are compromised and if an attacker is targeting a specific individual user account, with foreknowledge of data about that user, reuse of old passwords can cause a security breach. Using this policy setting with the Enforce password history setting prevents the easy 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 also 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.
4.2.4	Types of password 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 tools to discover the accounts and passwords.

4.2.5	The Passwords must meet complexity requirements policy setting determines whether passwords must meet a series of guidelines that are considered important for a strong password. Enabling this policy setting requires passwords to meet the following requirements: 1. Passwords may not contain the user's samAccountName (Account Name) value or entire displayName (Full Name value). Both checks are not case sensitive. The samAccountName is checked in its entirety only to determine whether it is part of the password. If the samAccountName is less than three characters long, this check is skipped. The displayName is parsed for delimiters: commas, periods, dashes or hyphens, underscores, spaces, pound signs, and tabs. If any of these delimiters are found, the displayName is split and all parsed sections (tokens) are confirmed to not be included in the password. Tokens that are less than three characters are ignored, and substrings of the tokens are not checked. For example, the name "Erin M. Hagens" is split into three tokens: "Erin", "M", and "Hagens". Because the second token is only one character long, it is ignored. Therefore, this user could not have a password that included either "erin" or "hagens" as a substring anywhere in the password. 2. The password contains characters from three of the following categories: • Uppercase letters of European languages (A through Z, with diacritic marks, Greek and Cyrillic characters) • Lowercase letters of European languages (a through z, sharp-s, with diacritic marks, Greek and Cyrillic characters) • Base 10 digits (0 through 9) • Non-alphanumeric characters (special characters) (for example, !, $, #, %) • Any Unicode character that is categorized as an alphabetic character but is not uppercase or lowercase. This includes Unicode characters from Asian languages. Complexity requirements are enforced when passwords are changed or created. The rules that are included in the Windows Server password complexity requirements are part of Passfilt.dll, and they cannot be directly modified. Enabling the default Passfilt.dll may cause some additional Help Desk calls for locked-out accounts because users might not be used to having passwords that contain characters other than those found in the alphabet. However, this policy setting is liberal enough that all users should be able to abide by the requirements with a minor learning curve. Additional settings that can be included in a custom Passfilt.dll are the use of non–upper-row characters. Upper-row characters are those that are typed by holding down the SHIFT key and typing any of the digits from 1 through 10.
4.2.6	Enabling this policy setting allows the operating system to store passwords in a weaker format that is much more susceptible to compromise and weakens your system security.

4.3.1	A Denial of Service (DoS) condition can be created if an attacker abuses the Account lockout threshold and repeatedly attempts to log on with a specific account. Once 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.
4.3.2	Password attacks can use automated methods to try millions of password combinations for any user account. The effectiveness of such attacks can be almost eliminated if you limit the number of failed logons that can be performed.However, a DoS attack could be performed on a domain that has an account lockout threshold configured. An 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 might be able to lock out every account.
4.3.3	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.

9.2 User Rights

Reference	Vulnerability
4.7.1	If an account is given this right the user of the account may create an application that calls into Credential Manager and is returned the credentials for another user.
4.7.2	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, then anyone in the group will be able to read the files in those shared folders.
4.7.3	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.
4.7.4	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. In the wrong hands, this privilege could be used to start a denial of service (DoS) attack.
4.7.5	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 run malicious software to elevate their privileges.

4.7.6	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 run malicious software to elevate their privileges.
4.7.7	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.
4.7.8	The default configuration for the Bypass traverse checking setting is to allow all users, including the Everyone group, to bypass traverse checking. Permissions to files and folders are controlled though appropriate configuration of file system access control lists (ACLs), as the ability to traverse the folder does not provide any read or write permissions to the user. 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, the administrator 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.
4.7.9	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. The risk from these types of events is mitigated on most domain controllers, member servers, and end-user computers because the Windows Time service automatically synchronizes time with domain controllers in the following ways: • All client desktop computers and member servers use the authenticating domain controller as their inbound time partner. • All domain controllers in a domain nominate the primary domain controller (PDC) emulator operations master as their inbound time partner. • All PDC emulator operations masters follow the hierarchy of domains in the selection of their inbound time partner. • The PDC emulator operations master at the root of the domain is authoritative for the organization. Therefore it is recommended that you configure this computer to synchronize with a reliable external time server. This vulnerability becomes much more serious if an attacker is able to change the system time and then stop the Windows Time service or reconfigure it to synchronize with a time server that is not accurate.
4.7.10	Changing the time zone represents little vulnerability because the system time is not affected. This setting merely enables users to display their preferred time zone while being synchronized with domain controllers in different time zones.

4.7.11	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.
4.7.12	A user account that is given this user right has complete control over the system and can lead to the system being compromised. It is highly recommended that you do not assign any user accounts this right. 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. Users 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.
4.7.13	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.
4.7.14	Users who have the Create permanent shared objects user right could create new shared objects and expose sensitive data to the network.
4.7.15	Users who have the Create Symbolic Links user right could inadvertently or maliciously expose your system to symbolic link attacks. Symbolic link attacks can be used to change the permissions on a file, to corrupt data, to destroy data, or as a Denial of Service attack.
4.7.16	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 insert rootkit code. By default, the Debug programs user right is assigned only to administrators, which helps to mitigate the risk from this vulnerability.
4.7.17	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.
4.7.18	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.
4.7.19	Accounts that can log on as a service could be used to configure and start new unauthorized services, such as a keylogger or other malicious software. The benefit of the specified countermeasure is somewhat reduced 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.
4.7.20	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, unauthorized users might download and run malicious software that elevates their privileges.

4.7.21	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, unauthorized users might download and run malicious software that elevates their privileges.
4.7.22	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.
4.7.23	Any user who can shut down a computer could cause a DoS condition to occur. Therefore, this user right should be tightly restricted.
4.7.24	An attacker could use this capability to create a large number of audited events, which would make it more difficult for a system administrator to locate any illicit activity. Also, if the event log is configured to overwrite events as needed, any evidence of unauthorized activities could be overwritten by a large number of unrelated events.
4.7.25	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.
4.7.26	This right is granted to all users by default. However, increasing the working set size for a process decreases the amount of physical memory available to the rest of the system. It would be possible for malicious code to increase the process working set to a level that could severely degrade system performance and potentially cause a denial of service.
4.7.27	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.
4.7.28	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.
4.7.29	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.
4.7.30	The Log on as a batch job user right presents a low-risk vulnerability. For most organizations, the default settings are sufficient.
4.7.31	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.
4.7.32	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.
4.7.33	By modifying the integrity label of an object owned by another user a malicious user may cause them to execute code at a higher level of privilege than intended.

4.7.34	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.
4.7.35	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.
4.7.36	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.
4.7.37	The Profile system performance user right poses a moderate vulnerability. Attackers with this user right could monitor a computer's performance to help identify critical processes that they might wish to attack directly. Attackers 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.
4.7.38	Anyone who has the Remove computer from docking station user right can log on and then remove a portable computer from its docking station. If this setting is not defined, it has the same effect as if everyone was granted this right. However, the value of implementing this countermeasure is reduced by the following factors: • If attackers can restart the computer, they could remove it from the docking station after the BIOS starts but before the operating system starts. • 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.
4.7.39	Users with the Replace a process level token privilege are able to start processes as other users whose credentials they know. They could use this method to hide their unauthorized actions on the computer. (On Windows 2000-based 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 in this section.)
4.7.40	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. Attackers could overwrite executable files that are used by legitimate administrators or system services with versions that include malicious software to grant themselves elevated privileges, compromise data, or install backdoors for continued access to the computer. Note: Even if the following 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.

4.7.41	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 which accounts and groups 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.
4.7.42	Any users 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.

9.3 Security Options

Reference	Vulnerability
4.8.1	Maintenance issues can arise under certain circumstances if you disable the Administrator account. For example, if the secure channel between a member computer and the domain controller fails in a domain environment for any reason and there is no other local Administrator account, you must restart in safe mode to fix the problem that broke the secure channel. If the current Administrator password does not meet the password requirements, you will not be able to re-enable the Administrator account after it is disabled. If this situation occurs, another member of the Administrators group must set the password on the Administrator account with the Local Users and Groups tool.
4.8.2	All network users will need to authenticate before they can access shared resources. If you disable the Guest account and the Network Access: Sharing and Security Model option is set to Guest Only, network logons, such as those performed by the Microsoft Network Server (SMB Service), will fail. This policy setting should have little impact on most organizations because it is the default setting in Microsoft Windows® 2000, Windows XP, and Windows Server™ 2003.
4.8.3	None. This is the default configuration.
4.8.4	You will have to inform users who are authorized to use this account of the new account name. (The guidance for this setting assumes that the Administrator account was not disabled, which was recommended earlier in this chapter.)
4.8.5	There should be little impact, because the Guest account is disabled by default.

4.8.6	If you enable the Audit: Audit the access of global system objects setting, a large number of security events could be generated, especially on busy domain controllers and application servers. Such an occurrence could cause servers to respond slowly and force the Security log to record numerous events of little significance. This policy setting can only be enabled or disabled, and there is no way to choose which events are recorded. Even organizations that have the resources to analyze events that are generated by this policy setting would not likely have the source code or a description of what each named object is used for. Therefore, it is unlikely that many organizations could benefit by enabling this policy setting.
4.8.7	If you enable this policy setting, a large number of security events could be generated, which could cause servers to respond slowly and force the Security event log to record numerous events of little significance. If you increase the Security log size to reduce the chances of a system shutdown, an excessively large log file may affect system performance.
4.8.8	The individual audit policy subcategories that are available in Windows Vista are not exposed in the interface of Group Policy tools. Administrators can deploy a custom audit policy that applies detailed security auditing settings to Windows Vista-based client computers in a Windows Server 2003 domain or in a Windows 2000 domain. If after enabling this setting, you attempt to modify an auditing setting by using Group Policy, the Group Policy auditing setting will be ignored in favor of the custom policy setting. To modify auditing settings by using Group Policy, you must first disable this key. Important Be very cautious about audit settings that can generate a large volume of traffic. For example, if you enable either success or failure auditing for all of the Privilege Use subcategories, the high volume of audit events generated can make it difficult to find other types of entries in the Security log. Such a configuration could also have a significant impact on system performance.
4.8.9	If you enable this policy setting, the administrative burden can be significant, especially if you also configure the Retention method for the Security log to Do not overwrite events (clear log manually). This configuration causes a repudiation threat (a backup operator could deny that they backed up or restored data) to become a denial of service (DoS) vulnerability, because a server could be forced to shut down if it is overwhelmed with logon events and other security events that are written to the Security log. Also, because the shutdown is not graceful, it is possible that irreparable damage to the operating system, applications, or data could result. Although the NTFS file system guarantees its integrity when an ungraceful computer shutdown occurs, it cannot guarantee that every data file for every application will still be in a usable form when the computer restarts.

4.8.10	Windows operating systems implement default COM ACLs when they are installed. Modifying these ACLs from the default may cause some applications or components that communicate by using DCOM to fail. If you implement a COM server and you override the default security settings, confirm that the application-specific call permissions ACL assigns correct permission to appropriate users. If it does not, you need to change your application-specific permission ACL to provide appropriate users with activation rights so that applications and Windows components that use DCOM do not fail.
4.8.11	Windows operating systems implement default COM ACLs when they are installed. Modifying these ACLs from the default may cause some applications to components that communicate by using DCOM to fail. If you implement a COM server and you override the default security settings, confirm that the application-specific launch permissions ACL assigns activation permission to appropriate users. If it does not, you need to change your application-specific launch permission ACL to provide appropriate users with activation rights so that applications and Windows components that use DCOM do not fail.
4.8.12	Users who have docked their computers will have to log on to the local console before they can undock their computers. For computers that do not have docking stations, this policy setting will have no impact.
4.8.13	Only Administrators will be able to format and eject removable media. If users are in the habit of using removable media for file transfers and storage, they will need to be informed of the change in policy.
4.8.14	Only users with Administrative, Power User, or Server Operator privileges will be able to install printers on the servers. If this policy setting is enabled but the driver for a network printer already exists on the local computer, users can still add the network printer.
4.8.15	Users who connect to the server over the network will not be able to use any CD drives that are installed on the server whenever anyone is logged on to the local console of the server. System tools that require access to the CD drive will fail. For example, the Volume Shadow Copy service attempts to access all CD and floppy disk drives that are present on the computer when it initializes, and if the service cannot access one of these drives, it will fail. This condition will cause the Windows Backup tool to fail if volume shadow copies were specified for the backup job. Any non-Microsoft backup products that use volume shadow copies will also fail. This policy setting would not be suitable for a computer that serves as a CD jukebox for network users.
4.8.16	Users who connect to the server over the network will not be able to use any floppy disk drives that are installed on the server whenever anyone is logged on to the local console of the server. System tools that require access to floppy disk drives will fail. For example, the Volume Shadow Copy service attempts to access all CD-ROM and floppy disk drives present on the computer when it initializes, and if the service cannot access one of these drives it will fail. This condition will cause the Windows Backup tool to fail if volume shadow copies were specified for the backup job. Any non-Microsoft backup products that use volume shadow copies will also fail.

4.8.17	Digital encryption and signing of the “secure channel” is a good idea where it is supported. The secure channel protects domain credentials as they are sent to the domain controller. However, only Windows NT 4.0 with Service Pack 6a (SP6a) and subsequent versions of the Windows operating system support digital encryption and signing of the secure channel. Windows 98 Second Edition clients do not support it unless they have the Dsclient installed. Therefore, you cannot enable the Domain member: Digitally encrypt or sign secure channel data (always) setting on domain controllers that support Windows 98 clients as members of the domain. Potential impacts can include the following: • The ability to create or delete trust relationships with clients running versions of Windows earlier than Windows NT 4.0 with SP6a will be disabled. • Logons from clients running versions of Windows earlier than Windows NT 4.0 with SP6a will be disabled. • The ability to authenticate other domains’ users from a domain controller running a version of Windows earlier than Windows NT 4.0 with SP6a in a trusted domain will be disabled. You can enable this policy setting after you eliminate all Windows 9x clients from the domain and upgrade all Windows NT 4.0 servers and domain controllers from trusted/trusting domains to Windows NT 4.0 with SP6a. You can enable the other two policy settings, Domain member: Digitally encrypt secure channel data (when possible) and Domain member: Digitally encrypt sign channel data (when possible), on all computers in the domain that support them and clients running versions of Windows earlier than Windows NT 4.0 with SP6a and applications that run on these versions of Windows will not be affected.
4.8.18	Digital encryption and signing of the “secure channel” is a good idea where it is supported. The secure channel protects domain credentials as they are sent to the domain controller. However, only Windows NT 4.0 Service Pack 6a (SP6a) and subsequent versions of the Windows operating system support digital encryption and signing of the secure channel. Windows 98 Second Edition clients do not support it unless they have the Dnsclient installed. Therefore, you cannot enable the Domain member: Digitally encrypt or sign secure channel data (always) setting on domain controllers that support Windows 98 clients as members of the domain. Potential impacts can include the following:

4.8.19	Digital encryption and signing of the “secure channel” is a good idea where it is supported. The secure channel protects domain credentials as they are sent to the domain controller. However, only Windows NT 4.0 with Service Pack 6a (SP6a) and subsequent versions of the Windows operating system support digital encryption and signing of the secure channel. Windows 98 Second Edition clients do not support it unless they have the Dsclient installed. Therefore, you cannot enable the Domain member: Digitally encrypt or sign secure channel data (always) setting on domain controllers that support Windows 98 clients as members of the domain. Potential impacts can include the following: • The ability to create or delete trust relationships with clients running versions of Windows earlier than Windows NT 4.0 with SP6a will be disabled. • Logons from clients running versions of Windows earlier than Windows NT 4.0 with SP6a will be disabled. • The ability to authenticate other domains’ users from a domain controller running a version of Windows earlier than Windows NT 4.0 with SP6a in a trusted domain will be disabled. You can enable this policy setting after you eliminate all Windows 9x clients from the domain and upgrade all Windows NT 4.0 servers and domain controllers from trusted/trusting domains to Windows NT 4.0 with SP6a. You can enable the other two policy settings, Domain member: Digitally encrypt secure channel data (when possible) and Domain member: Digitally encrypt sign channel data (when possible), on all computers in the domain that support them and clients running versions of Windows earlier than Windows NT 4.0 with SP6a and applications that run on these versions of Windows will not be affected.
4.8.20	None. This is the default configuration.
4.8.21	None. This is the default configuration.
4.8.22	Computers that have this policy setting enabled will not be able to join Windows NT 4.0 domains, and trusts between Active Directory domains and Windows NT-style domains may not work properly. Also, computers that do not support this policy setting will not be able to join domains in which the domain controllers have this policy setting enabled.
4.8.23	Users will always have to type their user names when they log on to the servers.
4.8.24	Unless they use a smart card to log on, users will have to simultaneously press three keys before the logon dialog box will display.
4.8.25	Users will see a message in a dialog box before they can log on to the server console. Note Windows Vista and Windows XP Professional support logon banners that can exceed 512 characters in length and that can also contain carriage-return line-feed sequences. However, Windows 2000-based clients cannot interpret and display these messages. You must use a Windows 2000-based computer to create a logon message policy that applies to Windows 2000-based computers. If you inadvertently create a logon message policy on a Windows Vista-based or Windows XP Professional-based computer and you discover that it does not display properly on Windows 2000-based computers, do the following: Change the setting to Not Defined, and then change the setting to the desired value by using a Windows 2000-based computer. Important If you do not reconfigure this setting to Not Defined before reconfiguring the setting using a Windows 2000-based computer, the changes will not take effect properly.

4.8.26	Users will see a message in a dialog box before they can log on to the server console. Note Windows Vista and Windows XP Professional support logon banners that can exceed 512 characters in length and that can also contain carriage-return line-feed sequences. However, Windows 2000-based clients cannot interpret and display these messages. You must use a Windows 2000-based computer to create a logon message policy that applies to Windows 2000-based computers. If you inadvertently create a logon message policy on a Windows Vista-based or Windows XP Professional-based computer and you discover that it does not display properly on Windows 2000-based computers, do the following: Change the setting to Not Defined, and then change the setting to the desired value by using a Windows 2000-based computer. Important If you do not reconfigure this setting to Not Defined before reconfiguring the setting using a Windows 2000-based computer, the changes will not take effect properly.
4.8.27	Users will be unable to log on to any computers if there is no domain controller available to authenticate them. Organizations may want to configure this value to 2 for end-user computers, especially for mobile users. A configuration value of 2 means that the user's logon information will still be in the cache, even if a member of the IT department has recently logged on to their computer to perform system maintenance. This method allows users to log on to their computers when they are not connected to the organization's network.
4.8.28	Users will see a dialog box prompt to change their password each time that they log on to the domain when their password is configured to expire in 14 or fewer days.
4.8.29	When the console on a computer is locked, either by a user or automatically by a screen saver time-out, the console can only be unlocked if the user is able to re-authenticate to the domain controller. If no domain controller is available, then users cannot unlock their workstations. If you configure the Interactive logon: Number of previous logons to cache (in case domain controller is not available) setting to 0, users whose domain controllers are unavailable (such as mobile or remote users) will not be able to log on.
4.8.30	All users of a computer with this setting enabled will have to use smart cards to log onto the local computer, which means that the organization will need a reliable public key infrastructure (PKI) as well as smart cards and smart card readers for these users. These requirements are significant challenges, because expertise and resources are required to plan for and deploy these technologies. However, Windows Server 2008 includes Certificate Services, a highly advanced service for implementing and managing certificates. When Certificate Services is combined with Windows 7 or Windows Vista, features such as automatic user and computer enrollment and renewal become available. For more information about deploying Smart Cards with Windows Vista see the paper "Windows Vista Smart Card Infrastructure" available for download at the Microsoft Web site (http://www.microsoft.com/downloads/details.aspx?FamilyID=ac201438-3317-44d3-9638-07625fe397b9&displaylang=en).

4.8.31	If you select Force Logoff, users will have to re-insert their smart cards and re-enter their PINs when they return to their workstations. Enforcing this setting on computers used by people who must log onto multiple computers in order to perform their duties could be frustrating and lower productivity. For example, if network administrators are limited to a single account but need to log into several computers simultaneously in order to effectively manage the network enforcing this setting will limit them to logging onto one computer at a time. For these reasons Microsoft recommends that this setting only be enforced on workstations used for purposes commonly associated with typical users such as document creation and email.
4.8.32	The Windows 2000 Server, Windows 2008 Server, Windows Server 2003, Windows XP Professional and Windows Vista implementations of the SMB file and print sharing protocol support mutual authentication, which prevents session hijacking attacks and supports message authentication to prevent man-in-the-middle attacks. SMB signing provides this authentication by placing a digital signature into each SMB, which is then verified by both the client and the server. Implementation of SMB signing may negatively affect performance, because each packet needs to be signed and verified. If these settings are enabled on a server that is performing multiple roles, such as a small business server that is serving as a domain controller, file server, print server, and application server performance may be substantially slowed. Additionally, if you configure computers to ignore all unsigned SMB communications, older applications and operating systems will not be able to connect. However, if you completely disable all SMB signing, computers will be vulnerable to session hijacking attacks. When SMB signing policies are enabled on domain controllers running Windows Server 2003 and member computers running Windows Vista SP1 or Windows Server 2008 group policy processing will fail. A hotfix is available from Microsoft that resolves this issue; see Microsoft Knowledgebase Article 950876 for more details: http://support.microsoft.com/default.aspx/kb/950876/.

4.8.33	The Windows 2000 Server, Windows 2000 Professional, Windows Server 2003, Windows XP Professional and Windows Vista implementations of the SMB file and print sharing protocol support mutual authentication, which prevents session hijacking attacks and supports message authentication to prevent man-in-the-middle attacks. SMB signing provides this authentication by placing a digital signature into each SMB, which is then verified by both the client and the server. Implementation of SMB signing may negatively affect performance, because each packet needs to be signed and verified. If these settings are enabled on a server that is performing multiple roles, such as a small business server that is serving as a domain controller, file server, print server, and application server performance may be substantially slowed. Additionally, if you configure computers to ignore all unsigned SMB communications, older applications and operating systems will not be able to connect. However, if you completely disable all SMB signing, computers will be vulnerable to session hijacking attacks. When SMB signing policies are enabled on domain controllers running Windows Server 2003 and member computers running Windows Vista SP1 or Windows Server 2008 group policy processing will fail. A hotfix is available from Microsoft that resolves this issue; see Microsoft Knowledgebase Article 950876 for more details: http://support.microsoft.com/default.aspx/kb/950876/.
4.8.34	Some very old applications and operating systems such as MS-DOS, Windows for Workgroups 3.11, and Windows 95a may not be able to communicate with the servers in your organization by means of the SMB protocol.
4.8.35	There will be little impact because SMB sessions will be re-established automatically if the client resumes activity.
4.8.36	The Windows 2000 Server, Windows 2000 Professional, Windows Server 2003, Windows XP Professional and Windows Vista implementations of the SMB file and print sharing protocol support mutual authentication, which prevents session hijacking attacks and supports message authentication to prevent man-in-the-middle attacks. SMB signing provides this authentication by placing a digital signature into each SMB, which is then verified by both the client and the server. Implementation of SMB signing may negatively affect performance, because each packet needs to be signed and verified. If these settings are enabled on a server that is performing multiple roles, such as a small business server that is serving as a domain controller, file server, print server, and application server performance may be substantially slowed. Additionally, if you configure computers to ignore all unsigned SMB communications, older applications and operating systems will not be able to connect. However, if you completely disable all SMB signing, computers will be vulnerable to session hijacking attacks. When SMB signing policies are enabled on domain controllers running Windows Server 2003 and member computers running Windows Vista SP1 or Windows Server 2008 group policy processing will fail. A hotfix is available from Microsoft that resolves this issue; see Microsoft Knowledgebase Article 950876 for more details: http://support.microsoft.com/default.aspx/kb/950876/.

4.8.37	The Windows 2000 Server, Windows 2000 Professional, Windows Server 2003, Windows XP Professional and Windows Vista implementations of the SMB file and print sharing protocol support mutual authentication, which prevents session hijacking attacks and supports message authentication to prevent man-in-the-middle attacks. SMB signing provides this authentication by placing a digital signature into each SMB, which is then verified by both the client and the server. Implementation of SMB signing may negatively affect performance, because each packet needs to be signed and verified. If these settings are enabled on a server that is performing multiple roles, such as a small business server that is serving as a domain controller, file server, print server, and application server performance may be substantially slowed. Additionally, if you configure computers to ignore all unsigned SMB communications, older applications and operating systems will not be able to connect. However, if you completely disable all SMB signing, computers will be vulnerable to session hijacking attacks. When SMB signing policies are enabled on domain controllers running Windows Server 2003 and member computers running Windows Vista SP1 or Windows Server 2008 group policy processing will fail. A hotfix is available from Microsoft that resolves this issue; see Microsoft Knowledgebase Article 950876 for more details: http://support.microsoft.com/default.aspx/kb/950876/.
4.8.38	If logon hours are not used in your organization, this policy setting will have no impact. If logon hours are used, existing user sessions will be forcibly terminated when their logon hours expire.
4.8.39	All Windows operating systems support both a client-side SMB component and a server-side SMB component. This setting affects the server SMB behavior, and its implementation should be carefully evaluated and tested to prevent disruptions to file and print serving capabilities.
4.8.40	Disabled is the default configuration for this policy setting on member computers; therefore it will have no impact on them. The default configuration for domain controllers is Enabled. If you disable this policy setting on domain controllers, legacy computers may be unable to communicate with Windows Server 2003–based domains. For example, the following computers may not work: • Windows NT 4.0–based Remote Access Service servers. • Microsoft SQL Servers™ that run on Windows NT 3.x–based or Windows NT 4.0–based computers. • Remote Access Service or Microsoft SQL servers that run on Windows 2000–based computers and are located in Windows NT 3.x domains or Windows NT 4.0 domains.
4.8.41	It will be impossible to establish trusts with Windows NT 4.0–based domains. Also, client computers that run older versions of the Windows operating system such as Windows NT 3.51 and Windows 95 will experience problems when they try to use resources on the server.
4.8.42	It will be impossible to grant access to users of another domain across a one-way trust because administrators in the trusting domain will be unable to enumerate lists of accounts in the other domain. Users who access file and print servers anonymously will be unable to list the shared network resources on those servers; the users will have to authenticate before they can view the lists of shared folders and printers.

4.8.43	Users will be forced to enter passwords whenever they log on to their Passport account or other network resources that aren't accessible to their domain account. Testing has shown that clients running Windows Vista or Windows Server 2008 will be unable to connect to Distributed File System (DFS) shares in untrusted domains. Enabling this setting also makes it impossible to specify alternate credentials for scheduled tasks, this can cause a variety of problems. For example, some third party backup products will no longer work. This policy setting should have no impact on users who access network resources that are configured to allow access with their Active Directory–based domain account.
4.8.44	None. This is the default configuration.
4.8.45	This configuration will disable null session access over named pipes, and applications that rely on this feature or on unauthenticated access to named pipes will no longer function. For example, with Microsoft Commercial Internet System 1.0, the Internet Mail Service runs under the Inetinfo process. Inetinfo starts in the context of the System account. When Internet Mail Service needs to query the Microsoft SQL Server database, it uses the System account, which uses null credentials to access a SQL pipe on the computer that runs SQL Server. To avoid this problem, refer to the Microsoft Knowledge Base article "How to access network files from IIS applications," which is located at http://support.microsoft.com/default.aspx?scid=207671.
4.8.46	Remote management tools such as the Microsoft Baseline Security Analyzer and Microsoft Systems Management Server require remote access to the registry to properly monitor and manage those computers. If you remove the default registry paths from the list of accessible ones, such remote management tools could fail. Note: If you want to allow remote access, you must also enable the Remote Registry service.
4.8.47	Remote management tools such as the Microsoft Baseline Security Analyzer and Microsoft Systems Management Server require remote access to the registry to properly monitor and manage those computers. If you remove the default registry paths from the list of accessible ones, such remote management tools could fail. Note: If you want to allow remote access, you must also enable the Remote Registry service.

4.8.48	You can enable this policy setting to restrict null session access for unauthenticated users to all server pipes and shared folders except those that are listed in the NullSessionPipes and NullSessionShares entries. If you choose to enable this setting and are supporting Windows NT 4.0 domains, you should check if any of the named pipes are required to maintain trust relationships between the domains, and then add the pipe to the Network access: Named pipes that can be accessed anonymously: • COMNAP–SNA session access • COMNODE–SNA session access • SQL\QUERY–SQL instance access • SPOOLSS–Spooler service • LLSRPC–License Logging service • Netlogon–Net Logon service • Lsarpc–LSA access • Samr–Remote access to SAM objects • browser–Computer Browser service Previous to the release of Windows Server 2003 with Service Pack 1 (SP1) these named pipes were allowed anonymous access by default, but with the increased hardening in Windows Server 2003 with SP1 these pipes must be explicitly added if needed.
4.8.49	There should be little impact because this is the default configuration. Only authenticated users will have access to shared resources on the server.
4.8.50	None. This is the default configuration.
4.8.51	If you enable this policy setting, services running as Local System that use Negotiate will use the computer identity. This might cause some authentication requests between Windows operating systems to fail and log an error. If you do not configure this policy setting, services running as Local System that use Negotiate when reverting to NTLM authentication will authenticate anonymously. This was the behavior in previous versions of Windows.
4.8.52	Any applications that require NULL sessions for LocalSystem will not work as designed.
4.8.53	Disabling this setting will disallow the online identities to be able to authenticate to the domain joined machine in Windows 7.
4.8.54	If not selected, the encryption type will not be allowed. This setting may affect compatibility with client computers or services and applications. Multiple selections are permitted.
4.8.55	Earlier operating systems such as Windows 95, Windows 98, and Windows ME as well as some third-party applications will fail.
4.8.56	When a user's logon time expires, SMB sessions will terminate. The user will be unable to log on to the computer until their next scheduled access time commences.

4.8.57	Clients that do not support NTLMv2 authentication will not be able to authenticate in the domain and access domain resources by using LM and NTLM. Note: For information about a hotfix to ensure that this setting works in networks that include Windows NT 4.0-based computers along with Windows 2000, Windows XP, and Windows Server 2003-based computers, see article 305379, Authentication Problems in Windows 2000 with NTLM 2 Levels Above 2 in a Windows NT 4.0 Domain, in the Microsoft Knowledge Base (http://go.microsoft.com/fwlink/?LinkId=100907).
4.8.58	If you configure the server to require LDAP signatures you must also configure the client. If you do not configure the client it will not be able to communicate with the server, which could cause many features to fail, including user authentication, Group Policy, and logon scripts.
4.8.59	Client computers that are enforcing these settings will be unable to communicate with older servers that do not support them. This setting could impact Windows Clustering when applied to servers running Windows Server 2003, see "How to apply more restrictive security settings on a Windows Server 2003-based cluster server" at http://support.microsoft.com/default.aspx?scid=kb;en-us;891597 and "You receive an "Error 0x8007042b" error message when you add or join a node to a cluster if you use NTLM version 2 in Windows Server 2003" at http://support.microsoft.com/kb/890761/ for more information on possible issues and how to resolve them.
4.8.60	Older clients that do not support these security settings will be unable to communicate with the computer. This setting could impact Windows Clustering when applied to servers running Windows Server 2003, see "How to apply more restrictive security settings on a Windows Server 2003-based cluster server" at http://support.microsoft.com/default.aspx?scid=kb;en-us;891597 and "You receive an "Error 0x8007042b" error message when you add or join a node to a cluster if you use NTLM version 2 in Windows Server 2003" at http://support. microsoft.com/kb/890761/ for more information on possible issues and how to resolve them.
4.8.61	If you configure this policy setting, you can define a list of remote servers to which clients are allowed to use NTLM authentication. If you do not configure this policy setting, no exceptions will be applied.
4.8.62	If you configure this policy setting, you can define a list of servers in this domain to which clients are allowed to use NTLM authentication. If you do not configure this policy setting, no exceptions will be applied.
4.8.63	If you select "Disable", or do not configure this policy setting, the server will not log events for incoming NTLM traffic. If you select "Enable auditing for domain accounts", the server will log events for NTLM pass-through authentication requests that would be blocked when the "Network Security: Restrict NTLM: Incoming NTLM traffic" policy setting is set to the "Deny all domain accounts" option. If you select "Enable auditing for all accounts", the server will log events for all NTLM authentication requests that would be blocked when the "Network Security: Restrict NTLM: Incoming NTLM traffic" policy setting is set to the "Deny all accounts" option.

4.8.64	If you select "Disable" or do not configure this policy setting, the domain controller will not log events for NTLM authentication in this domain. If you select "Enable for domain accounts to domain servers," the domain controller will log events for NTLM authentication logon attempts for domain accounts to domain servers when NTLM authentication would be denied because "Deny for domain accounts to domain servers" is selected in the "Network security: Restrict NTLM: NTLM authentication in this domain" policy setting. If you select "Enable for domain accounts," the domain controller will log events for NTLM authentication logon attempts that use domain accounts when NTLM authentication would be denied because "Deny for domain accounts" is selected in the "Network security: Restrict NTLM: NTLM authentication in this domain" policy setting. If you select "Enable for domain servers" the domain controller will log events for NTLM authentication requests to all servers in the domain when NTLM authentication would be denied because "Deny for domain servers" is selected in the "Network security: Restrict NTLM: NTLM authentication in this domain" policy setting. If you select "Enable all" the domain controller will log events for NTLM pass-through authentication requests from its servers and for its accounts which would be denied because "Deny all" is selected in the "Network security: Restrict NTLM: NTLM authentication in this domain" policy setting.
4.8.65	If you select "Allow all" or do not configure this policy setting, the server will allow all NTLM authentication requests. If you select "Deny all domain accounts," the server will deny NTLM authentication requests for domain logon and display an NTLM blocked error, but allow local account logon. If you select "Deny all accounts," the server will deny NTLM authentication requests from incoming traffic and display an NTLM blocked error.
4.8.66	If you select "Disabled" or do not configure this policy setting, the domain controller will allow all NTLM pass-through authentication requests within the domain. If you select "Deny for domain accounts to domain servers" the domain controller will deny all NTLM authentication logon attempts to all servers in the domain that are using domain accounts and return an NTLM blocked error unless the server name is on the exception list in the "Network security: Restrict NTLM: Add server exceptions for NTLM authentication in this domain" policy setting. If you select "Deny for domain account" the domain controller will deny all NTLM authentication logon attempts from domain accounts and return an NTLM blocked error unless the server name is on the exception list in the "Network security: Restrict NTLM: Add server exceptions for NTLM authentication in this domain" policy setting. If you select "Deny for domain servers" the domain controller will deny NTLM authentication requests to all servers in the domain and return an NTLM blocked error unless the server name is on the exception list in the "Network security: Restrict NTLM: Add server exceptions for NTLM authentication in this domain" policy setting. If you select "Deny all," the domain controller will deny all NTLM pass-through authentication requests from its servers and for its accounts and return an NTLM blocked error unless the server name is on the exception list in the "Network security: Restrict NTLM: Add server exceptions for NTLM authentication in this domain" policy setting.

4.8.67	If you select "Allow all" or do not configure this policy setting, the client computer can authenticate identities to a remote server by using NTLM authentication. If you select "Audit all," the client computer logs an event for each NTLM authentication request to a remote server. This allows you to identify those servers receiving NTLM authentication requests from the client computer. If you select "Deny all," the client computer cannot authenticate identities to a remote server by using NTLM authentication. You can use the "Network security: Restrict NTLM: Add remote server exceptions for NTLM authentication" policy setting to define a list of remote servers to which clients are allowed to use NTLM authentication.
4.8.68	Users will have to enter a user name and password to access the Recovery Console.
4.8.69	Users who have started a server through the Recovery Console and logged in with the built-in Administrator account will not be able to copy files and folders to a floppy disk.
4.8.70	Operators will have to log on to servers to shut them down or restart them.
4.8.71	It will take longer to shut down and restart the server, especially on servers with large paging files. For a server with 2 gigabytes (GB) of RAM and a 2-GB paging file, this policy setting could increase the shutdown process by 20 to 30 minutes, or more. For some organizations, this downtime violates their internal service level agreements. Therefore, use caution before you implement this countermeasure in your environment.
4.8.72	Users will have to enter their password every time they access a key that is stored on their computer. For example, if users use an S-MIME certificate to digitally sign their e-mail they will be forced to enter the password for that certificate every time they send a signed e-mail message. For some organizations the overhead that is involved using this configuration may be too high. At a minimum, this setting should be set to User is prompted when the key is first used.
4.8.73	Client computers that have this policy setting enabled will be unable to communicate by means of digitally encrypted or signed protocols with servers that do not support these algorithms. Network clients that do not support these algorithms will not be able to use servers that require them for network communications. For example, many Apache-based Web servers are not configured to support TLS. If yoREu enable this setting, you also need to configure Internet Explorer to use TLS. This policy setting also affects the encryption level that is used for the Remote Desktop Protocol (RDP). The Remote Desktop Connection tool uses the RDP protocol to communicate with servers that run Terminal Services and client computers that are configured for remote control; RDP connections will fail if both computers are not configured to use the same encryption algorithms. To enable Internet Explore to use TLS 1. On the Internet Explorer Tools menu, click Internet Options. 2. Click the Advanced tab. 3. Select the Use TLS 1.0 check box. It is also possible to configure this policy setting through Group Policy or by using the Internet Explorer Administrators Kit.
4.8.74	All subsystems will be forced to observe case insensitivity. This configuration may confuse users who are familiar with any UNIX-based operating systems that are case-sensitive.

4.8.75	None. This is the default configuration.
4.8.76	Applications that rely on the POSIX subsystem will no longer operate. For example, Microsoft Services for Unix (SFU) installs an updated version of the POSIX subsystem that is required, so you would need to reconfigure this setting in a Group Policy for any servers that use SFU.
4.8.77	If you enable certificate rules, software restriction policies check a certificate revocation list (CRL) to ensure that the software's certificate and signature are valid. This checking process may negatively affect performance when signed programs start. To disable this feature you can edit the software restriction policies in the desired GPO. On the Trusted Publishers Properties dialog box, clear the Publisher and Timestamp check boxes.
4.8.78	Users that log on using the local Administrator account will be prompted for consent whenever a program requests an elevation in privilege.
4.8.79	If you enable this setting, ("User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop"), requests for elevation are automatically sent to the interactive desktop (not the secure desktop) and also appear on the remote administrator's view of the desktop during a Windows Remote Assistance session, and the remote administrator is able to provide the appropriate credentials for elevation. This setting does not change the behavior of the UAC elevation prompt for administrators
4.8.80	This is the default behavior. Administrators should be made aware that they will be prompted for consent.
4.8.81	Users will need to provide administrative passwords to be able to run programs with elevated privileges. This could cause an increased load on IT staff while the programs that are impacted are identified and standard operating procedures are modified to support least privilege operations.
4.8.82	Users will need to provide administrative passwords to be able to install programs.
4.8.83	Enabling this setting requires that you have a PKI infrastructure and that your Enterprise administrators have populated the Trusted Root Store with the certificates for the allowed applications. Some older applications are not signed and will not be able to be used in an environment that is hardened with this setting. You should carefully test your applications in a pre-production environment before implementing this setting. For information about the steps required to test application compatibility, make application compatibility fixes, and sign installer packages to prepare your organization for deployment of Windows Vista User Account Control, see Understanding and Configuring User Account Control in Windows Vista (http://go.microsoft.com/fwlink/?LinkID=79026). Control over the applications that are installed on the desktops and the hardware that is able to join your domain should provide similar protection from the vulnerability addressed by this setting. Additionally, the level of protection provided by this setting is not an assurance that all rogue applications will be found.

4.8.84	If the application that requests UIAccess meets the UIAccess setting requirements, Windows 7 starts the application with the ability to bypass most of the UIPI restrictions. If the application does not meet the security restrictions, the application will be started without UIAccess rights and can interact only with applications at the same or lower privilege level.
4.8.85	Users and administrators will need to learn to work with UAC prompts and adjust their work habits to use least privilege operations.
4.8.86	None. This is the default configuration.
4.8.87	None. This is the default configuration.
4.8.88	
4.10.1	Group Policies will be reapplied every time they are refreshed, which could have a slight impact on performance.
4.11.1	This policy setting does not prevent the client computer from printing to printers on the intranet or the Internet over HTTP. It only prohibits drivers that are not already installed locally from downloading.
4.11.2	If this policy setting is enabled, Windows is prevented from downloading providers; only the service providers cached in the local registry will display.
4.11.3	If you enable this policy setting, the client computer will not be able to print to Internet printers over HTTP. This policy setting affects the client side of Internet printing only. Regardless of how it is configured, a computer could act as an Internet Printing server and make its shared printers available through HTTP.
4.11.4	Internet searches will still send the search text and information about the search to Microsoft and the chosen search provider. If you select Classic Search, the Search Companion feature will be unavailable. You can select Classic Search by clicking Start, Search, Change Preferences, and then Change Internet Search Behavior.
4.11.5	The Web Publishing wizard is used to download a list of providers and allow users to publish content to the Web.
4.11.6	Microsoft uses information collected through the Customer Experience Improvement Program to detect software flaws so that they can be corrected more quickly, enabling this setting will reduce the amount of data Microsoft is able to gather for this purpose.
4.11.7	Users will not be able to download new or updated device drivers from Windows Update.
4.12.1	If you enable this setting, certain computer programs such as antivirus software and software distribution and monitoring software are also prevented from execution. You should evaluate the threat level to your environment that this setting is designed to safeguard against before you decide on a strategy to use this setting for your organization.
4.12.2	If you enable the Do not process the run once list setting you should experience minimal functionality loss for users in your environment, especially if the clients have been configured with all of your organization's standard software before you apply this setting through Group Policy. However, this configuration may prevent some setup and installation programs, such as Internet Explorer, from working properly.

4.12.3	If you enable this policy, or if it is not configured, the user is prompted for a password when the system resumes from sleep. If you disable this policy, the user is not prompted for a password when the system resumes from sleep.
4.13.1	If you enable this policy, or if it is not configured, the user is prompted for a password when the system resumes from sleep. If you disable this policy, the user is not prompted for a password when the system resumes from sleep.
4.14.1	Help desk and support personnel will not be able to proactively offer assistance, although they can still respond to user assistance requests.
4.15.1	RPC applications that do not authenticate unsolicited inbound connection requests may not work properly when this configuration is applied. Ensure you test applications before you deploy this policy setting throughout your environment. Although the Authenticated value for this policy setting is not completely secure, it can be useful for providing application compatibility in your environment.
4.15.2	Anonymous access to RPC services could result in accidental disclosure of information to unauthenticated users.
4.16.1	Users will have to manually launch setup or installation programs that are provided on removable media.
4.17.1	If you enable this policy, users will always be required to type in a user name and password to elevate. If you disable this policy, all local administrator accounts on the computer will be displayed so the user can choose one and enter the correct password.
4.17.2	If you disable or do not configure this policy setting, users can enter Windows credentials within the user’s desktop session, potentially allowing malicious code access to the user’s Windows credentials.
4.19.1	Mobile users who access printers and other shared devices on their home networks will not be able to leverage the ease of use provided by HomeGroup functionality.
4.21.1	If you enable this policy setting and set it to False, new remote shell connections will be rejected by the server. If you disable or do not configure this policy setting, new remote shell connections will be allowed.
4.22.1	Critical operating system updates and service packs will automatically download and install at 3:00 A.M. daily. Although each version of Windows is thoroughly tested before release, it is possible that problems will be discovered after the products are shipped. The Configure Automatic Updates setting can help you ensure that the computers in your environment will always have the most recent critical operating system updates and service packs installed.

4.22.2	If you enable this policy setting, the user's last shut down choice (Hibernate, Restart, etc.) is the default option in the Shut Down Windows dialog box, regardless of whether the 'Install Updates and Shut Down' option is available in the 'What do you want the computer to do?' list. If you disable or do not configure this policy setting, the 'Install Updates and Shut Down' option will be the default option in the Shut Down Windows dialog box if updates are available for installation at the time the user selects the Shut Down option in the Start menu.
4.22.3	If you disable this policy setting, the Install Updates and Shut Down option will display in the Shut Down Windows dialog box if updates are available when the user selects the Shut Down option in the Start menu.
4.22.4	If you enable this policy setting, the operating systems on the servers in your environment will restart themselves automatically. For critical servers this could lead to temporary but unexpected, DoS conditions.
4.22.5	Automatic Updates will not start until 10 minutes after the computer restarts.
4.22.6	Critical updates and service packs will have to be proactively managed by the organization's IT staff.
5.1.1	If a user forgets to lock their computer when they walk away its possible that a passerby will hijack it.
5.1.2	If a user forgets to lock their computer when they walk away its possible that a passerby will hijack it.
5.1.3	If a user forgets to lock their computer when they walk away its possible that a passerby will hijack it.
5.2.1	Due to default permissions unprivileged users have little ability to modify sensitive data in the registry, nevertheless, preventing them from using registry editing tools will ensure that they are unable to view or modify any data stored there except through the normal graphical tools. Note that the value of this countermeasure is diminished by the fact that the user may find a third party tool that allows him to do the same thing.
5.3.1	A file that is downloaded from a computer in the Internet or Restricted Sites zone may be moved to a location that makes it appear safe, like an intranet file share, and executed by an unsuspecting user.
5.3.2	A user might remove information that indicates a file came from an untrustworthy location.
5.3.3	Antivirus programs that do not perform on-access checks may not be able to scan downloaded files.
5.4.1	The built-in CD burning feature can be used to surreptitiously copy information that resides on the computer or on the network.
6.4.2	Users might download drivers that include malicious code.
6.5.1	If users are able to download and install device drivers there is a small chance that they will install a driver that reduces system stability. There is an even smaller possibility that they will install a driver that includes malicious code. These risks are very low because Microsoft requires vendors to test drivers extensively before they can be published on Windows Update.

6.7.1	Enabling this setting ensures that anyone who wakes an unattended computer from sleep state will have to provide logon credentials before they can access the system.
6.8.2	There is slight risk that a rogue administrator will gain access to another user's desktop session, however, they cannot connect to a user’s computer unannounced or control it without permission from the user. When an expert tries to connect, the user can still choose to deny the connection or give the expert view-only privileges. The user must explicitly click the Yes button to allow the expert to remotely control the workstation.
6.8.3	A user might be tricked and accept an unsolicited Remote Assistance offer from a malicious user.
6.13.1	If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users
4.13.2	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 Chapter 5, "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.
6.15.1	By default, domain joined computers can be joined to a HomeGroup. While resources on a domain-joined computer cannot be shared to the HomeGroup, information from the domain-joined computer can be leaked to other computers in the HomeGroup.
6.16.1	If you enable this policy setting, the password saving checkbox is disabled for Terminal Services clients and users will not be able to save passwords. If you enable this policy setting, the password saving checkbox is disabled for Terminal Services clients and users will not be able to save passwords
6.16.2	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 access 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. If this setting is enabled legitimate users will be unable to use Terminal Services or Remote Desktop, this could make it more difficult for help desk technicians to troubleshoot and resolve problems remotely. It would also make it impossible to use Terminal Services for hosting shared applications.
6.16.3	Data could be forwarded from the user's Terminal Server session to the user's local computer without any direct user interaction. Drive redirection will not be possible.

6.16.4	Users have the option to store both their username and password when they create a new Remote Desktop connection shortcut. If the server that runs Terminal Services allows users who have used this feature to log on to the server but not enter their password, then it is possible that an attacker who has gained physical access to the user's computer could connect to a Terminal Server through the Remote Desktop connection shortcut, even though they may not know the user's password. Users will always have to enter their password when they establish new Terminal Server sessions.
6.16.5	If Terminal Server client connections are allowed that use low level encryption, it is more likely that an attacker will be able to decrypt any captured Terminal Services network traffic. Clients that do not support 128-bit encryption will be unable to establish Terminal Server sessions.
6.20.1	Data execution prevention helps reduce the risk of certain classes of attacks by blocking the execution of code stored where the system only expects data to be stored. Date execution prevent can cause certain plug-in applications for Windows Explorer to fail.