Windows 7 Security Compliance

Data collected on: 08/01/2016
14:41:50

Computer Configuration (Enabled)

Policies

Windows Settings

Security Settings

Local Policies/User Rights Assignment

Policy	Setting
Access Credential Manager as a trusted caller	
Access this computer from the network	BUILTIN\Administrators, BUILTIN\Users
Act as part of the operating system	
Adjust memory quotas for a process	NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE, BUILTIN\Administrators
Allow log on locally	BUILTIN\Users, BUILTIN\Administrators
Bypass traverse checking	BUILTIN\Administrators, NT AUTHORITY\LOCAL SERVICE, NT AUTHORITY\NETWORK SERVICE, BUILTIN\Users
Change the system time	BUILTIN\Administrators, NT AUTHORITY\LOCAL SERVICE
Change the time zone	BUILTIN\Users, BUILTIN\Administrators, NT AUTHORITY\LOCAL SERVICE
Create a pagefile	BUILTIN\Administrators
Create global objects	NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE, NT AUTHORITY\SERVICE, BUILTIN\Administrators
Debug programs	BUILTIN\Administrators
Deny access to this computer from the network	BUILTIN\Guests
Deny log on as a batch job	BUILTIN\Guests
Deny log on locally	BUILTIN\Guests
Enable computer and user accounts to be trusted for delegation	
Force shutdown from a remote system	BUILTIN\Administrators
Generate security audits	NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE
Impersonate a client after authentication	NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE, NT AUTHORITY\SERVICE, BUILTIN\Administrators
Increase a process working set	NT AUTHORITY\LOCAL SERVICE, BUILTIN\Administrators
Increase scheduling priority	BUILTIN\Administrators

Load and unload device drivers	BUILTIN\Administrators
Lock pages in memory	
Manage auditing and security log	BUILTIN\Administrators
Modify firmware environment values	BUILTIN\Administrators
Perform volume maintenance tasks	BUILTIN\Administrators
Profile system performance	BUILTIN\Administrators, NT SERVICE\WdiServiceHost
Remove computer from docking station	BUILTIN\Users, BUILTIN\Administrators
Replace a process level token	NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE
Shut down the system	BUILTIN\Users, BUILTIN\Administrators
Take ownership of files or other objects	BUILTIN\Administrators

Local Policies/Security Options

Accounts

Policy	Setting
Accounts: Guest account status	Disabled
Accounts: Limit local account use of blank passwords to console logon only	Enabled

Audit

Policy	Setting
Audit: Shut down system immediately if unable to log security audits	Disabled

Devices

Policy	Setting
Devices: Allowed to format and eject removable media	Administrators and Interactive Users
Devices: Prevent users from installing printer drivers	Disabled

Interactive Logon

Policy	Setting
Interactive logon: Do not display last user name	Enabled
Interactive logon: Do not require CTRL+ALT+DEL	Disabled
Interactive logon: Number of previous logons to cache (in case domain controller is not available)	2 logons
Interactive logon: Prompt user to change password before expiration	7 days
Interactive logon: Require Domain Controller authentication to unlock workstation	Disabled

Microsoft Network Client

Policy	Setting

Microsoft network client: Digitally sign communications (always)	Enabled
Microsoft network client: Digitally sign communications (if server agrees)	Enabled
Microsoft network client: Send unencrypted password to third-party SMB servers	Disabled

Network Access

Policy	Setting
Network access: Allow anonymous SID/Name translation	Disabled
Network access: Do not allow anonymous enumeration of SAM accounts	Enabled
Network access: Do not allow anonymous enumeration of SAM accounts and shares	Enabled
Network access: Let Everyone permissions apply to anonymous users	Disabled
Network access: Remotely accessible registry paths	System\CurrentControlSet\Control\ProductOptions, System\CurrentControlSet\Control\Server Applications, Software\Microsoft\Windows NT\CurrentVersion
Network access: Remotely accessible registry paths and sub-paths	System\CurrentControlSet\Control\Print\Printers, System\CurrentControlSet\Services\Eventlog, Software\Microsoft\OLAP Server, Software\Microsoft\Windows NT\CurrentVersion\Print, Software\Microsoft\Windows NT\CurrentVersion\Windows, System\CurrentControlSet\Control\ContentIndex, System\CurrentControlSet\Control\Terminal Server, System\CurrentControlSet\Control\Terminal Server\UserConfig, System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration, Software\Microsoft\Windows NT\CurrentVersion\Perflib, System\CurrentControlSet\Services\SysmonLog
Network access: Restrict anonymous access to Named Pipes and Shares	Enabled
Network access: Shares that can be accessed anonymously	
Network access: Sharing and security model for local accounts	Classic - local users authenticate as themselves

Network Security

Policy	Setting
Network security: Do not store LAN Manager hash value on next password change	Enabled
Network security: LAN Manager authentication level	Send NTLMv2 response only. Refuse LM & NTLM
Network security: LDAP client signing requirements	Negotiate signing
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients	Enabled
Require NTLMv2 session security	Enabled
Require 128-bit encryption	Enabled
Network security: Minimum session security for NTLM SSP based (including secure RPC) servers	Enabled
Require NTLMv2 session security	Enabled
Require 128-bit encryption	Enabled

Shutdown

Policy	Setting
Shutdown: Clear virtual memory pagefile	Disabled

System Objects

Policy	Setting
System objects: Require case insensitivity for non-Windows subsystems	Enabled
System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)	Enabled

User Account Control

Policy	Setting
User Account Control: Admin Approval Mode for the Built-in Administrator account	Enabled
User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop	Disabled
User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode	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
User Account Control: Detect application installations and prompt for elevation	Enabled

User Account Control: Only elevate executables that are signed and validated	Disabled
User Account Control: Only elevate UIAccess applications that are installed in secure locations	Enabled
User Account Control: Run all administrators in Admin Approval Mode	Enabled
User Account Control: Switch to the secure desktop when prompting for elevation	Enabled
User Account Control: Virtualize file and registry write failures to per-user locations	Enabled

Other

Policy	Setting
Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings	Enabled
Domain member: Digitally encrypt or sign secure channel data (always)	Enabled
Domain member: Digitally encrypt secure channel data (when possible)	Enabled
Domain member: Digitally sign secure channel data (when possible)	Enabled
Domain member: Disable machine account password changes	Disabled
Domain member: Maximum machine account password age	30 days
Domain member: Require strong (Windows 2000 or later) session key	Enabled
Microsoft network server: Amount of idle time required before suspending session	15 minutes
Microsoft network server: Digitally sign communications (always)	Enabled
Microsoft network server: Digitally sign communications (if client agrees)	Enabled
Microsoft network server: Disconnect clients when logon hours expire	Enabled
Recovery console: Allow automatic administrative logon	Disabled

Registry Values

Policy	Setting

MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AutoAdminLogon	"0"
MACHINE\Software\Microsoft\Windows	"0"
NT\CurrentVersion\Winlogon\ScreenSaverGracePeriod	
MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\SafeDllSearchMode	1
MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Security\WarningLevel	90
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\DisableIPSourceRouting	2
MACHINE\System\CurrentControlSet\Services\Tcpip6\Parameters\DisableIPSourceRouting	2

System Services

Function Discovery Provider Host (Startup Mode: Automatic)

Permissions
No permissions specified

Auditing
No auditing specified

Function Discovery Resource Publication (Startup Mode: Automatic)

Permissions
No permissions specified

Auditing
No auditing specified

Windows Firewall with Advanced Security

Global Settings

Policy	Setting
Policy version	Not Configured
Disable stateful FTP	Not Configured
Disable stateful PPTP	Not Configured
IPsec exempt	Not Configured
IPsec through NAT	Not Configured
Preshared key encoding	Not Configured
SA idle time	Not Configured
Strong CRL check	Not Configured

Domain Profile Settings

Policy	Setting
Firewall state	Off
Inbound connections	Block
Outbound connections	Allow
Apply local firewall rules	Yes
Apply local connection security rules	Yes
Display notifications	Yes
Allow unicast responses	No
Log dropped packets	Not Configured
Log successful connections	Not Configured

Log file path	Not Configured
Log file maximum size (KB)	Not Configured

Private Profile Settings

Policy	Setting
Firewall state	On
Inbound connections	Block
Outbound connections	Allow
Apply local firewall rules	Yes
Apply local connection security rules	Yes
Display notifications	Yes
Allow unicast responses	No
Log dropped packets	Not Configured
Log successful connections	Not Configured
Log file path	Not Configured
Log file maximum size (KB)	Not Configured

Public Profile Settings

Policy	Setting
Firewall state	On
Inbound connections	Block
Outbound connections	Allow
Apply local firewall rules	Yes
Apply local connection security rules	No
Display notifications	No
Allow unicast responses	No
Log dropped packets	Not Configured
Log successful connections	Not Configured
Log file path	Not Configured
Log file maximum size (KB)	Not Configured

Connection Security Settings

Advanced Audit Configuration

Account Logon

Policy	Setting
Audit Credential Validation	Success, Failure
Audit Kerberos Authentication Service	No Auditing
Audit Kerberos Service Ticket Operations	No Auditing
Audit Other Account Logon Events	No Auditing

Account Management

Policy	Setting
Audit Application Group Management	No Auditing
Audit Computer Account Management	Success
Audit Distribution Group Management	No Auditing
Audit Other Account Management Events	Success, Failure
Audit Security Group Management	Success, Failure
Audit User Account Management	Success, Failure

Detailed Tracking

Policy	Setting
Audit DPAPI Activity	No Auditing
Audit Process Creation	Success
Audit Process Termination	No Auditing
Audit RPC Events	No Auditing

DS Access

Policy	Setting
Audit Detailed Directory Service Replication	No Auditing
Audit Directory Service Access	No Auditing
Audit Directory Service Changes	No Auditing
Audit Directory Service Replication	No Auditing

Logon/Logoff

Policy	Setting
Audit Account Lockout	No Auditing
Audit IPsec Extended Mode	No Auditing
Audit IPsec Main Mode	No Auditing
Audit IPsec Quick Mode	No Auditing
Audit Logoff	Success
Audit Logon	Success, Failure
Audit Network Policy Server	No Auditing
Audit Other Logon/Logoff Events	No Auditing
Audit Special Logon	Success

Object Access

Policy	Setting
Audit Application Generated	No Auditing
Audit Certification Services	No Auditing
Audit Detailed File Share	No Auditing
Audit File Share	No Auditing

Audit File System	No Auditing
Audit Filtering Platform Connection	No Auditing
Audit Filtering Platform Packet Drop	No Auditing
Audit Handle Manipulation	No Auditing
Audit Kernel Object	No Auditing
Audit Other Object Access Events	No Auditing
Audit Registry	No Auditing
Audit SAM	No Auditing

Policy Change

Policy	Setting
Audit Audit Policy Change	Success, Failure
Audit Authentication Policy Change	Success
Audit Authorization Policy Change	No Auditing
Audit Filtering Platform Policy Change	No Auditing
Audit MPSSVC Rule-Level Policy Change	No Auditing
Audit Other Policy Change Events	No Auditing

Privilege Use

Policy	Setting
Audit Non Sensitive Privilege Use	No Auditing
Audit Other Privilege Use Events	No Auditing
Audit Sensitive Privilege Use	Success, Failure

System

Policy	Setting
Audit IPsec Driver	Success, Failure
Audit Other System Events	No Auditing
Audit Security State Change	Success, Failure
Audit Security System Extension	Success, Failure
Audit System Integrity	Success, Failure

Administrative Templates

Policy definitions (ADMX files) retrieved from the central store.

Network/Network Connections/Windows Firewall/Domain Profile

Policy	Setting	Comment
Windows Firewall: Prohibit notifications	Disabled	
Windows Firewall: Prohibit unicast response to multicast or broadcast requests	Enabled	

Windows Firewall: Protect all network connections	Disabled

Network/Network Provider

Policy	Setting	Comment
Hardened UNC Paths	Enabled	

Specify hardened network paths. In the name field, type a fully-qualified UNC path for each network resource. To secure all access to a share with a particular name, regardless of the server name, specify a server name of '*' (asterisk). For example, "*\NETLOGON". To secure all access to all shares hosted on a server, the share name portion of the UNC path may be omitted. For example, "\\SERVER". In the value field, specify one or more of the following options, separated by commas: 'RequireMutualAuthentication=1': Mutual authentication between the client and server is required to ensure the client connects to the correct server. 'RequireIntegrity=1': Communication between the client and server must employ an integrity mechanism to prevent data tampering. 'RequirePrivacy=1': Communication between the client and the server must be encrypted to prevent third parties from observing sensitive data.

Hardened UNC Paths:	
*\SYSVOL	RequireMutualAuthentication=1, RequireIntegrity=1
*\NETLOGON	RequireMutualAuthentication=1, RequireIntegrity=1

You should require both Integrity and Mutual Authentication for any UNC paths that host executable programs, script files, or files that control security policies. Consider hosting files that do not require Integrity or Privacy on separate shares from those that absolutely need such security for optimal performance. For additional details on configuring Windows computers to require additional security when accessing specific UNC paths, visit http://support.microsoft.com/kb/3000483.

System/Group Policy

Policy	Setting	Comment
Configure registry policy processing	Enabled	
Do not apply during periodic background processing	Disabled	
Process even if the Group Policy objects have not changed	Enabled	

System/Internet Communication Management/Internet Communication settings

Policy	Setting	Comment
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

System/Remote Procedure Call

Policy	Setting	Comment
Enable RPC Endpoint Mapper Client Authentication	Disabled	
Restrict Unauthenticated RPC clients	Enabled	
RPC Runtime Unauthenticated Client Restriction to Apply:	Authenticated	

Windows Components/AutoPlay Policies

Policy	Setting	Comment
Turn off Autoplay	Enabled	
Turn off Autoplay on:	All drives	

Windows Components/Credential User Interface

Policy	Setting	Comment
Enumerate administrator accounts on elevation	Disabled	

Windows Components/Event Log Service/Application

Policy	Setting	Comment
Control Event Log behavior when the log file reaches its maximum size	Disabled	
Specify the maximum log file size (KB)	Enabled	
Maximum Log Size (KB)	32768	

Windows Components/Event Log Service/Security

Policy	Setting	Comment
Control Event Log behavior when the log file reaches its maximum size	Disabled	
Specify the maximum log file size (KB)	Enabled	

Maximum Log Size (KB)	81920

Windows Components/Event Log Service/System

Policy	Setting	Comment
Control Event Log behavior when the log file reaches its maximum size	Disabled	
Specify the maximum log file size (KB)	Enabled	
Maximum Log Size (KB)	32768	

Windows Components/File Explorer

Policy	Setting	Comment
Turn off Data Execution Prevention for Explorer	Disabled	

Windows Components/Remote Desktop Services/Remote Desktop Connection Client

Policy	Setting	Comment
Do not allow passwords to be saved	Enabled	

Windows Components/Remote Desktop Services/Remote Desktop Session Host/Security

Policy	Setting	Comment
Always prompt for password upon connection	Enabled	
Set client connection encryption level	Enabled	
Encryption Level	High Level	
Choose the encryption level from the drop-down list.		

Windows Components/Windows Installer

Policy	Setting	Comment
Always install with elevated privileges	Disabled	

Windows Components/Windows Remote Shell

Policy	Setting	Comment
Allow Remote Shell Access	Enabled	

Windows Components/Windows Update

Policy	Setting	Comment
Allow non-administrators to receive update notifications	Disabled	
Allow signed updates from an intranet Microsoft update service location	Enabled	
Configure Automatic Updates	Enabled	
Configure automatic updating:	4 - Auto download and schedule the install	

The following settings are only required and applicable if 4 is selected.	
Install during automatic maintenance	Disabled
Scheduled install day:	0 - Every day
Scheduled install time:	19:00

Policy	Setting	Comment
Do not display 'Install Updates and Shut Down' option in Shut Down Windows dialog box	Enabled	
Enabling Windows Update Power Management to automatically wake up the system to install scheduled updates	Enabled	
No auto-restart with logged on users for scheduled automatic updates installations	Enabled	

User Configuration (Disabled)

No settings defined.