Configuration Security

for

Active Directory

Table of Contents

Summary 5

Specification 6

1.0 Local Policies 6

1.1 Local Policies\Audit Policy 6

1.2 Local Policies\User Rights Assignment 7

1.3 Local Policies\Security Options 9

1.4 Local Policies\Security Options 20

2.0 Security Settings 21

2.1 Security Settings\Event Log 21

2.2 Security Settings\Restricted Groups 22

2.3 Security Settings\System Services 22

3.0 Windows Firewall Properties 30

3.1 Windows Firewall Properties\Domain Profile Tab 30

3.2 Windows Firewall Properties\Private Profile Tab 30

3.3 Windows Firewall Properties\Public Profile Tab 31

4.0 Advanced Audit Policy Configuration 32

4.1 Advanced Audit Policy Configuration\Audit Policy\Account Logon 32

4.2 Advanced Audit Policy Configuration\Audit Policy\Account Management 32

4.3 Advanced Audit Policy Configuration\Audit Policy\Detailed Tracking 33

4.4 Advanced Audit Policy Configuration\Audit Policy\DS Access 33

4.5 Advanced Audit Policy Configuration\Audit Policy\Logon Logoff 34

4.6 Advanced Audit Policy Configuration\Audit Policy\Object Access 35

4.7 Advanced Audit Policy Configuration\Audit Policy\Policy Change 35

4.8 Advanced Audit Policy Configuration\Audit Policy\Privilege Use 36

4.9 Advanced Audit Policy Configuration\Audit Policy\Global Object Access Auditing 36

4.10 Advanced Audit Policy Configuration\Audit Policy\System 37

5.0 Network 38

5.1 Network\Windows Connect Now 38

5.2 Network\Link-Layer Topology Discovery 38

5.3 Network\Microsoft Peer-to-Peer Networking Services 38

5.4 Network\Network Connections 39

5.5 Network\Network Connections\Windows Firewall \Domain Profile 39

5.6 Network\Network Connections\Windows Firewall \Standard Profile 40

6.0 System 41

6.1 System\Group Policy 41

6.2 System\Internet Communication Management\Internet Communication settings 42

6.3 System\Logon 43

6.4 System\Power Management\Sleep Settings 43

6.5 System\Remote Assistance 43

6.6 System\Remote Procedure Call 44

6.7 System\Windows Time Service\Time Providers 44

6.8 System\Driver Installation 44

7.0 Event Log Service 45

7.1 Event Log Service\Application 45

7.2 Event Log Service\Security 45

7.3 Event Log Service\System 45

8.0 Internet Explorer 46

8.1 Internet Explorer 46

8.2 Internet Explorer\Internet Control Panel\Advanced Page 46

8.3 Internet Explorer\Security Features\Add-on Management 47

8.4 Internet Explorer\Security Features\Protection From Zone Elevation 47

8.5 Internet Explorer\Security Features\Restrict ActiveX Install 47

8.6 Internet Explorer\Security Features\Restrict File Download 48

8.7 Internet Explorer\Security Features\Scripted Window Security Restrictions 48

8.8 Internet Explorer\Security Features\Consistent Mime Handling 48

8.9 Internet Explorer\Security Features\Mime Sniffing Safety Feature 48

8.10 Internet Explorer\Security Features\MK Protocol Security Restriction 49

9.0 Windows Components 49

9.1 Windows Components\NetMeeting 49

9.2 Windows Components\Online Assistance 49

9.3 Windows Components\Remote Desktop Services\Remote Desktop Connection Client 49

9.4 Windows Components\Remote Desktop Services\Remote Desktop Session Host\Session Time Limits 50

9.5 Windows Components\Remote Desktop Services\Remote Desktop Session Host\Temporary folders 50

9.6 Windows Components\Remote Desktop Services\Remote Desktop Session Host\Connections 51

9.7 Windows Components\Remote Desktop Services\Remote Desktop Session Host\Device and Resource Redirection 51

9.8 Windows Components\Remote Desktop Services\Remote Desktop Session Host\Printer Redirection 52

9.9 Windows Components\Remote Desktop Services\Remote Desktop Session Host\Remote Session Environment 52

9.10 Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security 52

9.11 Windows Components\RSS Feeds 53

9.12 Windows Components\AutoPlay Policies 53

9.13 Windows Components\Windows Defender 54

9.14 Windows Components\Windows Error Reporting 54

9.15 Windows Components\Windows Explorer 54

9.16 Windows Components\Windows Installer 55

9.17 Windows Components\Windows Logon Options 55

9.18 Windows Components\Windows Mail 55

9.19 Windows Components\Windows Media Digital Rights Management 56

9.20 Windows Components\Windows Media Player 56

9.21 Windows Components\Windows Messenger 56

9.22 Windows Components\Windows PowerShell 57

9.23 Windows Components\Windows Remote Management (WinRM)\WinRM Client 57

9.24 Windows Components\Windows Remote Management (WinRM)\WinRM Service 58

9.25 Windows Components\Windows Remote Shell 58

9.26 Windows Components\Windows Update 59

9.27 Windows Components\Credential User Interface 60

Authority/Responsibility 61

Definitions/Terms/Acronyms 61

References 61

Constraints/Waivers 61

Implementation Plan 61

# Summary

This specification plan describes the items that, at a minimum, must be evaluated by ITI with oversight by Global Cyber Security for incorporation into a formal security specification for this technology. During that evaluation ITI and Global Cyber Security will note any issues of concern for determination of applicability and compliance by Global Cyber Security.

ITI with oversight by Global Cyber Security will determine the appropriate technology to monitor compliance with the specification. If applicable, as determined by Global Cyber Security, items from CIS benchmarks designated as Level 1, Scorable must be monitored. If a particular CIS benchmark does not exist or does not provide level and scorablity designations, then a previous version or an alternate ranking source as deemed appropriate by Global Cyber Security may be used to determine the priority of monitoring for a particular item.

This specification plan applies to Active Directory Configuration implementations.

|  |  |  |
| --- | --- | --- |
|

|  |  |
| --- | --- |
|

|  |
| --- |
| Specification |

 |

 |

Active Directory Configuration

# Local Policies

## 1.1 Local Policies\Audit Policy

|  |  |
| --- | --- |
| **1.1.2.4.2.1** | **Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Audit Policy** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Audit Account Logon Events | Should be | Not Defined | Domain Controllers |
|   | 2 | Audit Account Management | Should be | Not Defined | Domain Controllers |
|   | 3 | Audit Directory Service Access | Should be | Not Defined | Domain Controllers |
|   | 4 | Audit Logon Events | Should be | Not Defined | Domain Controllers |
|   | 5 | Audit Object Access | Should be | Not Defined | Domain Controllers |
|   | 6 | Audit Policy Change | Should be | Not Defined | Domain Controllers |
|   | 7 | Audit Privilege Use | Should be | Not Defined | Domain Controllers |
|   | 8 | Audit Process Tracking | Should be | Not Defined | Domain Controllers |
|   | 9 | Audit System Events | Should be | Not Defined | Domain Controllers |

## 1.2 Local Policies\User Rights Assignment

|  |  |
| --- | --- |
| **1.1.2.4.2.2** | **Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment** |
| **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
| 1 | Access Credential Manager As A Trusted Caller | Must be |   | Domain Controllers |
| 2 | Access This Computer From The Network | Must be | Administrators, Authenticated Users, Enterprise Domain Controllers; Read-only Domain Controllers | Domain Controllers |
| 3 | Act As Part Of The Operating System | Must be | No One | Domain Controllers |
| 4 | Add Workstations To Domain | Must be | Administrators | Domain Controllers |
| 5 | Adjust Memory Quotas For A Process | Must be | Administrators, Local Service, Network Service | Domain Controllers |
| 6 | Allow Log On Locally | Must be | Administrators | Domain Controllers |
| 7 | Allow Log On Through Remote Desktop Services | Must be | Administrators; Enterprise Admins; Domain Admins | Domain Controllers |
| 8 | Back Up Files And Directories | Must be | Administrators | Domain Controllers |
| 9 | Bypass Traverse Checking | Must be | Administrators, Authenticated Users, Local Service, Network Service | Domain Controllers |
| 10 | Change The System Time | Must be | Local Service, Administrators | Domain Controllers |
| 11 | Change The Time Zone | Must be | Local Service, Administrators | Domain Controllers |
| 12 | Create A Page file | Must be | Administrators | Domain Controllers |
| 13 | Create A Token Object | Must be | No One | Domain Controllers |
| 14 | Create Global Objects | Must be | Administrators, Service, Local Service, Network Service | Domain Controllers |
| 15 | Create Permanent Shared Objects | Must be | No One | Domain Controllers |
| 16 | Create Symbolic Links | Must be | Administrators | Domain Controllers |
| 17 | Debug Programs | Must be | Administrators | Domain Controllers |
| 18 | Deny Access To This Computer From The Network | Must be | Guest; Support\_388945a0; Ngdc\_gst | Domain Controllers |
| 19 | Deny Log On As A Batch Job | Must be | Guest; Support\_388945a0; Ngdc\_gst | Domain Controllers |
| 20 | Deny Log On As A Service | Must be | Guest; Support\_388945a0; Ngdc\_gst | Domain Controllers |
| 21 | Deny Log On Locally | Must be | Guest; Support\_388945a0; Ngdc\_gst | Domain Controllers |
| 22 | Deny Log On Through Remote Desktop Services | Must be | Guest; Support\_388945a0; Ngdc\_gst | Domain Controllers |
| 23 | Enable Computer And User Accounts To Be Trusted For Delegation | Must be | Administrators | Domain Controllers |
| 24 | Force Shutdown From A Remote System | Must be | Administrators | Domain Controllers |
| 25 | Generate Security Audits | Must be | Local Service, Network Service | Domain Controllers |
| 26 | Impersonate A Client After Authentication | Must be | Administrators, Service, Local Service, Network Service | Domain Controllers |
| 27 | Increase A Process Working Set | Must be | Administrators, Local Service | Domain Controllers |
| 28 | Increase Scheduling Priority | Must be | Administrators | Domain Controllers |
| 29 | Load And Unload Device Drivers | Must be | Administrators | Domain Controllers |
| 30 | Lock Pages In Memory | Must be | No One | Domain Controllers |
| 31 | Log On As A Batch Job | Must be | Administrators | Domain Controllers |
| 32 | Log On As A Service | Should be | Not Defined | Domain Controllers |
| 33 | Manage Auditing And Security Log | Must be | Administrators, Exchange Servers, Administrators, Exchange Enterprise Servers, americas\$fimsvc001 | Domain Controllers |
| 34 | Modify An Object Label | Must be | No One | Domain Controllers |
| 35 | Modify Firmware Environment Values | Must be | Administrators | Domain Controllers |
| 36 | Perform Volume Maintenance Tasks | Must be | Administrators | Domain Controllers |
| 37 | Profile Single Process | Must be | Administrators | Domain Controllers |
| 38 | Profile System Performance | Should be | Not Defined | Domain Controllers |
| 39 | Remove Computer From Docking Station | Must be | Administrators | Domain Controllers |
| 40 | Replace A Process Level Token | Must be | Local Service, Network Service | Domain Controllers |
| 41 | Restore Files And Directories | Must be | Administrators | Domain Controllers |
| 42 | Shut Down The System | Must be | Administrators | Domain Controllers |
| 43 | Synchronize Directory Service Data | Should be | Not Defined | Domain Controllers |
| 44 | Take Ownership Of Files Or Other Objects | Must be | Administrators | Domain Controllers |

## 1.3 Local Policies\Security Options

|  |  |
| --- | --- |
| **1.1.2.4.2.3** | **Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options** |
| **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
| 1 | Accounts: Administrator Account Status | Should be | Not Defined | Domain Controllers |
| 2 | Accounts: Guest Account Status | Must be | Disabled | Domain Controllers |
| 3 | Accounts: Limit Local Account Use Of Blank Passwords To Console Logon Only | Must be | Enabled | Domain Controllers |
| 4 | Accounts: Rename Administrator Account | Must be | Imsupport | Domain Controllers |
| 5 | Accounts: Rename Guest Account | Must be | Ngdc\_gst | Domain Controllers |
| 6 | Audit: Audit The Access Of Global System Objects | Must be | Disabled | Domain Controllers |
| 7 | Audit: Audit The Use Of Backup And Restore Privilege | Must be | Disabled | Domain Controllers |
| 8 | Audit: Force Audit Policy Subcategory Settings (windows Vista Or Later) To Override Audit Policy Category Settings | Must be | Enabled | Domain Controllers |
| 9 | Audit: Shut Down System Immediately If Unable To Log Security Audits | Must be | Disabled | Domain Controllers |
| 10 | Dcom: Machine Access Restrictions In Security Descriptor Definition Language (sddl) Syntax | Should be | Not Defined | Domain Controllers |
| 11 | Dcom: Machine Launch Restrictions In Security Descriptor Definition Language (sddl) Syntax | Should be | Not Defined | Domain Controllers |
| 12 | Devices: Allow Undock Without Having To Log On | Must be | Disabled | Domain Controllers |
| 13 | Devices: Allowed To Format And Eject Removable Media | Must be | Administrators | Domain Controllers |
| 14 | Devices: Prevent Users From Installing Printer Drivers | Must be | Enabled | Domain Controllers |
| 15 | Devices: Restrict Cd-rom Access To Locally Logged-on User Only | Must be | Enabled | Domain Controllers |
| 16 | Devices: Restrict Floppy Access To Locally Logged-on User Only | Must be | Enabled | Domain Controllers |
| 17 | Domain Controller: Allow Server Operators To Schedule Tasks | Must be | Disabled | Domain Controllers |
| 18 | Domain Controller: Ldap Server Signing Requirements | Must be | Require Signing | Domain Controllers |
| 19 | Domain Controller: Refuse Machine Account Password Changes | Must be | Disabled | Domain Controllers |
| 20 | Domain Member: Digitally Encrypt Or Sign Secure Channel Data (always) | Must be | Enabled | Domain Controllers |
| 21 | Domain Member: Digitally Encrypt Secure Channel Data (when Possible) | Must be | Enabled | Domain Controllers |
| 22 | Domain Member: Digitally Sign Secure Channel Data (when Possible) | Must be | Enabled | Domain Controllers |
| 23 | Domain Member: Disable Machine Account Password Changes | Must be | Disabled | Domain Controllers |
| 24 | Domain Member: Maximum Machine Account Password Age | Must be | 30 | Domain Controllers |
| 25 | Domain Member: Require Strong (windows 2000 Or Later) Session Key | Must be | Enabled | Domain Controllers |
| 26 |  Schanel Protocols: Ssl 2.0 Client | Must be | Disabled | Domain Controllers |
| 27 |  Schanel Protocols: Ssl 2.0 Server | Must be | Disabled | Domain Controllers |
| 28 |  Schannel Ciphers: Des 56 | Must be | Disabled | Domain Controllers |
| 29 |  Schannel Ciphers: Null | Must be | Disabled | Domain Controllers |
| 30 |  Schannel Ciphers: Rc2 128 | Must be | Disabled | Domain Controllers |
| 31 |  Schannel Ciphers: Rc2 40 | Must be | Disabled | Domain Controllers |
| 32 |  Schannel Ciphers: Rc2 56 | Must be | Disabled | Domain Controllers |
| 33 |  Schannel Ciphers: Rc4 40 | Must be | Disabled | Domain Controllers |
| 34 |  Schannel Ciphers: Rc4 56 | Must be | Disabled | Domain Controllers |
| 35 |  Schannel Ciphers: Rc4 64 | Must be | Disabled | Domain Controllers |
| 36 | Interactive Logon: Display User Information When The Session Is Locked | Must be | User Display Name, Domain And User Names | Domain Controllers |
| 37 | Interactive Logon: Do Not Display Last User Name | Must be | Enabled | Domain Controllers |
| 38 | Interactive Logon: Do Not Require Ctrl+alt+del | Must be | Disabled | Domain Controllers |
| 39 | Interactive Logon: Message Text For Users Attempting To Log On | Must be | This computing system is a company owned asset and provided for the exclusive use of authorized personnel for business purposes. All information and data created, accessed, processed, or stored using this system (including personal information) are subject to monitoring, auditing, or review to the extent permitted by applicable law. Unauthorized use or abuse of this system may lead to corrective action including termination of employment, civil and/or criminal penalties. | Domain Controllers |
| 40 | Interactive Logon: Message Title For Users Attempting To Log On | Must be | Terms of Use | Domain Controllers |
| 41 | Interactive Logon: Number Of Previous Logons To Cache (in Case Domain Controller Is Not Available) | Must be | 10 Logons | Domain Controllers |
| 42 | Interactive Logon: Prompt User To Change Password Before Expiration | Must be | 10 Days | Domain Controllers |
| 43 | Interactive Logon: Require Domain Controller Authentication To Unlock Workstation | Must be | Disabled | Domain Controllers |
| 44 | Interactive Logon: Require Smart Card | Should be | Not Defined | Domain Controllers |
| 45 | Interactive Logon: Smart Card Removal Behavior | Must be | Lock Workstation | Domain Controllers |
| 46 | Microsoft Network Client: Digitally Sign Communications (always) | Must be | Disabled | Domain Controllers |
| 47 | Microsoft Network Client: Digitally Sign Communications (if Server Agrees) | Must be | Enabled | Domain Controllers |
| 48 | Microsoft Network Client: Send Unencrypted Password To Third-party Smb Servers | Must be | Disabled | Domain Controllers |
| 49 | Microsoft Network Server: Amount Of Idle Time Required Before Suspending Session | Must be | 15 | Domain Controllers |
| 50 | Microsoft Network Server: Digitally Sign Communications (always) | Must be | Disabled | Domain Controllers |
| 51 | Microsoft Network Server: Digitally Sign Communications (if Client Agrees) | Must be | Enabled | Domain Controllers |
| 52 | Microsoft Network Server: Disconnect Clients When Logon Hours Expire | Must be | Enabled | Domain Controllers |
| 53 | Microsoft Network Server: Server Spn Target Name Validation Level | Should be | Not Defined | Domain Controllers |
| 54 | Mss: (autoadminlogon) Enable Automatic Logon (not Recommended) | Must be | Disabled | Domain Controllers |
| 55 | Mss: (autoreboot) Allow Windows To Automatically Restart After A System Crash (recommended Except For Highly Secure Environments) | Should be | Not Defined | Domain Controllers |
| 56 | Mss: (autoshareserver) Enable Administrative Shares (recommended Except For Highly Secure Environments) | Must be | Enabled | Domain Controllers |
| 57 | Mss: (disableipsourcerouting Ipv6) Ip Source Routing Protection Level (protects Against Packet Spoofing) | Must be | Highest Protection, Source Routing Is Completely Disabled | Domain Controllers |
| 58 | Mss: (disableipsourcerouting) Ip Source Routing Protection Level (protects Against Packet Spoofing) | Must be | Highest Protection, Source Routing Is Completely Disabled | Domain Controllers |
| 59 | Mss: (disablesavepassword) Prevent The Dial-up Passsword From Being Saved (recommended) | Must be | Enabled | Domain Controllers |
| 60 | Mss: (enabledeadgwdetect) Allow Automatic Detection Of Dead Network Gateways (could Lead To Dos) | Must be | Disabled | Domain Controllers |
| 61 | Mss: (enableicmpredirect) Allow Icmp Redirects To Override Ospf Generated Routes | Must be | Disabled | Domain Controllers |
| 62 | Mss: (hidden) Hide Computer From The Browse List (not Recommended Except For Highly Secure Environments) | Must be | Disabled | Domain Controllers |
| 63 | Mss: (keepalivetime) How Often Keep-alive Packets Are Sent In Milliseconds | Must be | 300000 Or 5 Minutes (recommended) | Domain Controllers |
| 64 | Mss: (nodefaultexempt) Configure Ipsec Exemptions For Various Types Of Network Traffic | Should be | Not Defined | Domain Controllers |
| 65 | Mss: (nonamereleaseondemand) Allow The Computer To Ignore Netbios Name Release Requests Except From Wins Servers | Must be | Enabled | Domain Controllers |
| 66 | Mss: (ntfsdisable8dot3namecreation) Enable The Computer To Stop Generating 8.3 Style Filenames (recommended) | Should be | Not Defined | Domain Controllers |
| 67 | Mss: (performrouterdiscovery) Allow Irdp To Detect And Configure Default Gateway Addresses (could Lead To Dos) | Must be | Disabled | Domain Controllers |
| 68 | Mss: (safedllsearchmode) Enable Safe Dll Search Mode (recommended) | Must be | Enabled | Domain Controllers |
| 69 | Mss: (screensavergraceperiod) The Time In Seconds Before The Screen Saver Grace Period Expires (0 Recommended) | Must be | 0 | Domain Controllers |
| 70 | Mss: (synattackprotect) Syn Attack Protection Level (protects Against Dos) | Must be | Connections Time Out Sooner If A Syn Attack Is Detected | Domain Controllers |
| 71 | Mss: (tcpmaxconnectresponseretransmissions) Syn-ack Retransmissions When A Connection Request Is Not Acknowledged | Must be | 3 & 6 Seconds, Half-open Connections Dropped After 21 Seconds | Domain Controllers |
| 72 | Mss: (tcpmaxdataretransmissions) How Many Times Unacknowledged Data Is Retransmitted (3 Recommended, 5 Is Default) | Must be | 3 | Domain Controllers |
| 73 | Mss: (tcpmaxdataretransmissions) Ipv6 How Many Times Unacknowledged Data Is Retransmitted (3 Recommended, 5 Is Default) | Must be | 3 | Domain Controllers |
| 74 | Mss: (warninglevel) Percentage Threshold For The Security Event Log At Which The System Will Generate A Warning | Must be | 90 | Domain Controllers |
| 75 | Network Access: Allow Anonymous Sid/name Translation | Must be | Disabled | Domain Controllers |
| 76 | Network Access: Do Not Allow Anonymous Enumeration Of Sam Accounts | Must be | Enabled | Domain Controllers |
| 77 | Network Access: Do Not Allow Anonymous Enumeration Of Sam Accounts And Shares | Must be | Enabled | Domain Controllers |
| 78 | Network Access: Do Not Allow Storage Of Passwords And Credentials For Network Authentication | Must be | Disabled | Domain Controllers |
| 79 | Network Access: Let Everyone Permissions Apply To Anonymous Users | Must be | Disabled | Domain Controllers |
| 80 | Network Access: Named Pipes That Can Be Accessed Anonymously | Should be | Not Defined | Domain Controllers |
| 81 | Network Access: Remotely Accessible Registry Paths | Must be | System\currentcontrolset\control\productoptionsSystem\currentcontrolset\control\server ApplicationsSoftware\microsoft\windows Nt\currentversion | Domain Controllers |
| 82 | Network Access: Remotely Accessible Registry Paths And Sub-paths | Must be | System\currentcontrolset\control\print\printersSystem\currentcontrolset\services\eventlogSoftware\microsoft\olap ServerSoftware\microsoft\windows Nt\currentversion\printSoftware\microsoft\windows Nt\currentversion\windowsSystem\currentcontrolset\control\contentindexSystem\currentcontrolset\control\terminal ServerSystem\currentcontrolset\control\terminal Server\userconfigSystem\currentcontrolset\control\terminal Server\defaultuserconfigurationSoftware\microsoft\windows Nt\currentversion\perflibSystem\currentcontrolset\services\sysmonlog | Domain Controllers |
| 83 | Network Access: Restrict Anonymous Access To Named Pipes And Shares | Must be | Enabled | Domain Controllers |
| 84 | Network Access: Shares That Can Be Accessed Anonymously | Must be | None | Domain Controllers |
| 85 | Network Access: Sharing And Security Model For Local Accounts | Must be | Classic - Local Users Authenticate As Themselves | Domain Controllers |
| 86 | Network Security: Allow Local System To Use Computer Identity For Ntlm | Should be | Not Defined | Domain Controllers |
| 87 | Network Security: Allow Localsystem Null Session Fallback | Must be | Enabled | Domain Controllers |
| 88 | Network Security: Allow Pku2u Authentication Requests To This Computer To Use Online Identities | Must be | Disabled | Domain Controllers |
| 89 | Network Security: Configure Encryption Types Allowed For Kerberos | Must be | Rc4\_hmac\_md5,aes128\_hmac\_sha1,aes256\_hmac\_sha1,future Encryption Types | Domain Controllers |
| 90 | Network Security: Do Not Store Lan Manager Hash Value On Next Password Change | Must be | Enabled | Domain Controllers |
| 91 | Network Security: Force Logoff When Logon Hours Expire | Must be | Disabled | Domain Controllers |
| 92 | Network Security: Lan Manager Authentication Level | Must be | Send Ntlmv2 Responses Only | Domain Controllers |
| 93 | Network Security: Ldap Client Signing Requirements | Must be | Negotiate Signing | Domain Controllers |
| 94 | Network Security: Minimum Session Security For Ntlm Ssp Based (including Secure Rpc) Clients | Must be | Require 128-bit Encryption | Domain Controllers |
| 95 | Network Security: Minimum Session Security For Ntlm Ssp Based (including Secure Rpc) Servers | Must be | Require 128-bit Encryption | Domain Controllers |
| 96 | Network Security: Restrict Ntlm: Add Remote Server Exceptions For Ntlm Authentication | Should be | Not Defined | Domain Controllers |
| 97 | Network Security: Restrict Ntlm: Add Server Exceptions In This Domain | Should be | Not Defined | Domain Controllers |
| 98 | Network Security: Restrict Ntlm: Audit Incoming Ntlm Traffic | Should be | Not Defined | Domain Controllers |
| 99 | Network Security: Restrict Ntlm: Audit Ntlm Authentication In This Domain | Should be | Not Defined | Domain Controllers |
| 100 | Network Security: Restrict Ntlm: Incoming Ntlm Traffic | Should be | Not Defined | Domain Controllers |
| 101 | Network Security: Restrict Ntlm: Ntlm Authentication In This Domain | Should be | Not Defined | Domain Controllers |
| 102 | Network Security: Restrict Ntlm: Outgoing Ntlm Traffic To Remote Servers | Should be | Not Defined | Domain Controllers |
| 103 | Recovery Console: Allow Automatic Administrative Logon | Must be | Disabled | Domain Controllers |
| 104 | Recovery Console: Allow Floppy Copy And Access To All Drives And All Folders | Must be | Enabled | Domain Controllers |
| 105 | Shutdown: Allow System To Be Shut Down Without Having To Log On | Must be | Disabled | Domain Controllers |
| 106 | Shutdown: Clear Virtual Memory Pagefile | Must be | Disabled | Domain Controllers |
| 107 | System Cryptography: Force Strong Key Protection For User Keys Stored On The Computer | Must be | User Is Prompted When The Key Is First Used | Domain Controllers |
| 108 | System Cryptography: Use Fips Compliant Algorithms For Encryption, Hashing, And Signing | Must be | Disabled | Domain Controllers |
| 109 | System Objects: Require Case Insensitivity For Non-windows Subsystems | Must be | Enabled | Domain Controllers |
| 110 | System Objects: Strengthen Default Permissions Of Internal System Objects (e.g. Symbolic Links) | Must be | Enabled | Domain Controllers |
| 111 | System Settings: Optional Subsystems | Must be | None | Domain Controllers |
| 112 | System Settings: Use Certificate Rules On Windows Executables For Software Restriction Policies | Should be | Not Defined | Domain Controllers |
| 113 | User Account Control: Admin Approval Mode For The Built-in Administrator Account | Must be | Enabled | Domain Controllers |
| 114 | User Account Control: Allow Uiaccess Applications To Prompt For Elevation Without Using The Secure Desktop | Must be | Disabled | Domain Controllers |
| 115 | User Account Control: Behavior Of The Elevation Prompt For Administrators In Admin Approval Mode | Must be | Prompt For Consent For Non-windows Binaries | Domain Controllers |
| 116 | User Account Control: Behavior Of The Elevation Prompt For Standard Users | Must be | Prompt For Credentials On The Secure Desktop | Domain Controllers |
| 117 | User Account Control: Detect Application Installations And Prompt For Elevation | Must be | Disabled | Domain Controllers |
| 118 | User Account Control: Only Elevate Executables That Are Signed And Validated | Must be | Disabled | Domain Controllers |
| 119 | User Account Control: Only Elevate Uiaccess Applications That Are Installed In Secure Locations | Must be | Enabled | Domain Controllers |
| 120 | User Account Control: Run All Administrators In Admin Approval Mode | Must be | Enabled | Domain Controllers |
| 121 | User Account Control: Switch To The Secure Desktop When Prompting For Elevation | Must be | Enabled | Domain Controllers |
| 122 | User Account Control: Virtualize File And Registry Write Failures To Per-user Locations | Must be | Enabled | Domain Controllers |

## 1.4 Local Policies\Security Options

|  |  |
| --- | --- |
| **1.1.2.4.2.4** | **Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Microsoft Network Server: Disconnect Clients When Logon Hours Expire | Must be | Enabled | Domain Controllers |

# 2.0 Security Settings

## 2.1 Security Settings\Event Log

|  |  |
| --- | --- |
| **1.1.2.4.3** | **Computer Configuration\Policies\Windows Settings\Security Settings\Event Log** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Maximum Application Log Size | Should be | Not Defined | Domain Controllers |
|   | 2 | Maximum Security Log Size | Should be | Not Defined | Domain Controllers |
|   | 3 | Maximum System Log Size | Should be | Not Defined | Domain Controllers |
|   | 4 | Retain Application Log | Should be | Not Defined | Domain Controllers |
|   | 5 | Retain Security Log | Should be | Not Defined | Domain Controllers |
|   | 6 | Retain System Log | Should be | Not Defined | Domain Controllers |

## 2.2 Security Settings\Restricted Groups

|  |  |
| --- | --- |
| **1.1.2.4.4** | **Computer Configuration\Policies\Windows Settings\Security Settings\Restricted Groups** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Backup Operators | Should be | Not Defined | Domain Controllers |
|   | 2 | Power Users | Should be | Not Defined | Domain Controllers |
|   | 3 | Remote Desktop Users | Should be | Not Defined | Domain Controllers |
|   | 4 | Users | Should be | Not Defined | Domain Controllers |

## 2.3 Security Settings\System Services

|  |  |
| --- | --- |
| **1.1.2.4.5** | **Computer Configuration\Policies\Windows Settings\Security Settings\System Services** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Active Directory Certificate Services | Must be | Disabled | Domain Controllers |
|   | 2 | Active Directory Domain Services | Should be | Not Defined | Domain Controllers |
|   | 3 | Active Directory Web Services | Should be | Not Defined | Domain Controllers |
|   | 4 | Ad Fs Web Agent Authentication Service | Should be | Not Defined | Domain Controllers |
|   | 5 | Ad Rms Logging Service | Should be | Not Defined | Domain Controllers |
|   | 6 | Application Experience | Should be | Not Defined | Domain Controllers |
|   | 7 | Application Host Helper Service | Should be | Not Defined | Domain Controllers |
|   | 8 | Application Identity | Should be | Not Defined | Domain Controllers |
|   | 9 | Application Information | Should be | Not Defined | Domain Controllers |
|   | 10 | Application Layer Gateway Service | Should be | Not Defined | Domain Controllers |
|   | 11 | Application Management | Should be | Not Defined | Domain Controllers |
|   | 12 | Asp .net State Service | Must be | Disabled | Domain Controllers |
|   | 13 | Background Intelligent Transfer Service | Must be | Automatic | Domain Controllers |
|   | 14 | Base Filtering Engine | Must be | Automatic | Domain Controllers |
|   | 15 | Bitlocker Drive Encryption Service | Should be | Not Defined | Domain Controllers |
|   | 16 | Bits Compact Server | Should be | Not Defined | Domain Controllers |
|   | 17 | Block Level Backup Engine Service | Should be | Not Defined | Domain Controllers |
|   | 18 | Branchcache | Should be | Not Defined | Domain Controllers |
|   | 19 | Certificate Propagation | Must be | Automatic | Domain Controllers |
|   | 20 | Client For Nfs | Must be | Disabled | Domain Controllers |
|   | 21 | Cluster Service | Should be | Not Defined | Domain Controllers |
|   | 22 | Cng Key Isolation | Should be | Not Defined | Domain Controllers |
|   | 23 | Com+ Event System | Must be | Automatic | Domain Controllers |
|   | 24 | Com+ System Application | Should be | Not Defined | Domain Controllers |
|   | 25 | Computer Browser | Should be | Not Defined | Domain Controllers |
|   | 26 | Credential Manager | Should be | Not Defined | Domain Controllers |
|   | 27 | Cryptographic Services | Must be | Automatic | Domain Controllers |
|   | 28 | Dcom Server Process Launcher | Must be | Automatic | Domain Controllers |
|   | 29 | Desktop Window Manager Session Manager | Must be | Automatic | Domain Controllers |
|   | 30 | Dfs Namespace | Should be | Not Defined | Domain Controllers |
|   | 31 | Dfs Replication | Should be | Not Defined | Domain Controllers |
|   | 32 | Dhcp Client | Should be | Not Defined | Domain Controllers |
|   | 33 | Dhcp Server | Must be | Disabled | Domain Controllers |
|   | 34 | Diagnostic Policy Service | Should be | Not Defined | Domain Controllers |
|   | 35 | Diagnostic Service Host | Should be | Not Defined | Domain Controllers |
|   | 36 | Diagnostic System Host | Should be | Not Defined | Domain Controllers |
|   | 37 | Disk Defragmenter | Should be | Not Defined | Domain Controllers |
|   | 38 | Distributed Link Tracking Client | Must be | Disabled | Domain Controllers |
|   | 39 | Distributed Transaction Coordinator | Should be | Not Defined | Domain Controllers |
|   | 40 | Dns Client | Must be | Automatic | Domain Controllers |
|   | 41 | Dns Server | Should be | Not Defined | Domain Controllers |
|   | 42 | Encrypting File System | Should be | Not Defined | Domain Controllers |
|   | 43 | Extensible Authentication Protocol | Must be | Automatic | Domain Controllers |
|   | 44 | Fax Service | Must be | Disabled | Domain Controllers |
|   | 45 | File Replication | Should be | Not Defined | Domain Controllers |
|   | 46 | File Server Resource Manager | Should be | Not Defined | Domain Controllers |
|   | 47 | File Server Storage Reports Manager | Should be | Not Defined | Domain Controllers |
|   | 48 | Function Discovery Provider Host | Should be | Not Defined | Domain Controllers |
|   | 49 | Function Discovery Resource Publication | Should be | Not Defined | Domain Controllers |
|   | 50 | Group Policy Client | Must be | Automatic | Domain Controllers |
|   | 51 | Health Key And Certificate Management | Must be | Automatic | Domain Controllers |
|   | 52 | Human Interface Device Access | Should be | Not Defined | Domain Controllers |
|   | 53 | Iis Admin Service | Must be | Disabled | Domain Controllers |
|   | 54 | Ike And Authip Ipsec Keying Modules | Must be | Automatic | Domain Controllers |
|   | 55 | Indexing Service | Should be | Not Defined | Domain Controllers |
|   | 56 | Interactive Services Detection | Should be | Not Defined | Domain Controllers |
|   | 57 | Internet Connection Sharing (ics) | Must be | Disabled | Domain Controllers |
|   | 58 | Intersite Messaging | Should be | Not Defined | Domain Controllers |
|   | 59 | Ip Helper | Should be | Not Defined | Domain Controllers |
|   | 60 | Ipsec Policy Agent | Must be | Automatic | Domain Controllers |
|   | 61 | Kerberos Key Distribution Center | Should be | Not Defined | Domain Controllers |
|   | 62 | Ktmrm For Distributed Transaction Coordinator | Should be | Not Defined | Domain Controllers |
|   | 63 | Link-layer Topology Discovery Mapper | Should be | Not Defined | Domain Controllers |
|   | 64 | Lpd Service | Must be | Disabled | Domain Controllers |
|   | 65 | Message Queuing | Should be | Not Defined | Domain Controllers |
|   | 66 | Message Queuing Triggers | Should be | Not Defined | Domain Controllers |
|   | 67 | Microsoft .net Framework Ngen V2.0.50727\_i64 | Should be | Not Defined | Domain Controllers |
|   | 68 | Microsoft .net Framework Ngen V2.0.50727\_x64 | Should be | Not Defined | Domain Controllers |
|   | 69 | Microsoft .net Framework Ngen V2.0.50727\_x86 | Should be | Not Defined | Domain Controllers |
|   | 70 | Microsoft Fibre Channel Platform Registration Service | Must be | Automatic | Domain Controllers |
|   | 71 | Microsoft Ftp Service | Must be | Disabled | Domain Controllers |
|   | 72 | Microsoft Iscsi Initiator Service | Should be | Not Defined | Domain Controllers |
|   | 73 | Microsoft Isns Server | Should be | Not Defined | Domain Controllers |
|   | 74 | Microsoft Software Shadow Copy Provider | Should be | Not Defined | Domain Controllers |
|   | 75 | Multimedia Class Scheduler | Should be | Not Defined | Domain Controllers |
|   | 76 | Net.msmq Listener Adapter | Should be | Not Defined | Domain Controllers |
|   | 77 | Net.pipe Listener Adapter | Should be | Not Defined | Domain Controllers |
|   | 78 | Net.tcp Listener Adapter | Should be | Not Defined | Domain Controllers |
|   | 79 | Net.tcp Port Sharing Service | Should be | Not Defined | Domain Controllers |
|   | 80 | Netlogon | Should be | Not Defined | Domain Controllers |
|   | 81 | Network Access Protection Agent | Must be | Automatic | Domain Controllers |
|   | 82 | Network Connections | Should be | Not Defined | Domain Controllers |
|   | 83 | Network List Service | Must be | Automatic | Domain Controllers |
|   | 84 | Network Location Awareness | Must be | Automatic | Domain Controllers |
|   | 85 | Network Policy Server | Must be | Disabled | Domain Controllers |
|   | 86 | Network Store Interface Service | Must be | Automatic | Domain Controllers |
|   | 87 | Offline Files | Should be | Not Defined | Domain Controllers |
|   | 88 | Online Responder Service | Must be | Disabled | Domain Controllers |
|   | 89 | Peer Name Resolution Protocol | Must be | Disabled | Domain Controllers |
|   | 90 | Peer Networking Identity Manager | Must be | Disabled | Domain Controllers |
|   | 91 | Performance Counter Dll Host | Should be | Not Defined | Domain Controllers |
|   | 92 | Performance Logs & Alerts | Should be | Not Defined | Domain Controllers |
|   | 93 | Plug And Play | Must be | Automatic | Domain Controllers |
|   | 94 | Pnp-x Ip Bus Enumerator | Must be | Disabled | Domain Controllers |
|   | 95 | Pnrp Machine Name Publication Service | Must be | Disabled | Domain Controllers |
|   | 96 | Portable Device Enumerator Service | Should be | Not Defined | Domain Controllers |
|   | 97 | Power | Should be | Not Defined | Domain Controllers |
|   | 98 | Print Spooler | Should be | Not Defined | Domain Controllers |
|   | 99 | Problem Reports And Solutions Control Panel Support | Should be | Not Defined | Domain Controllers |
|   | 100 | Protected Storage | Should be | Not Defined | Domain Controllers |
|   | 101 | Quality Windows Audio Video Experience | Should be | Not Defined | Domain Controllers |
|   | 102 | Remote Access Auto Connection Manager | Should be | Not Defined | Domain Controllers |
|   | 103 | Remote Access Connection Manager | Should be | Not Defined | Domain Controllers |
|   | 104 | Remote Access Quarantine Agent | Must be | Disabled | Domain Controllers |
|   | 105 | Remote Desktop Configuration | Should be | Not Defined | Domain Controllers |
|   | 106 | Remote Desktop Connection Broker | Should be | Not Defined | Domain Controllers |
|   | 107 | Remote Desktop Gateway | Should be | Not Defined | Domain Controllers |
|   | 108 | Remote Desktop Licensing | Should be | Not Defined | Domain Controllers |
|   | 109 | Remote Desktop Services | Should be | Not Defined | Domain Controllers |
|   | 110 | Remote Desktop Services Usermode Port Redirector | Should be | Not Defined | Domain Controllers |
|   | 111 | Remote Desktop Virtualization Host | Should be | Not Defined | Domain Controllers |
|   | 112 | Remote Procedure Call (rpc) | Must be | Automatic | Domain Controllers |
|   | 113 | Remote Procedure Call (rpc) Locator | Should be | Not Defined | Domain Controllers |
|   | 114 | Remote Registry | Must be | Automatic | Domain Controllers |
|   | 115 | Removable Storage | Should be | Not Defined | Domain Controllers |
|   | 116 | Resultant Set Of Policy Provider | Should be | Not Defined | Domain Controllers |
|   | 117 | Routing And Remote Access | Must be | Disabled | Domain Controllers |
|   | 118 | Rpc Endpoint Mapper | Should be | Not Defined | Domain Controllers |
|   | 119 | Rpc/http Load Balancing Service | Should be | Not Defined | Domain Controllers |
|   | 120 | Secondary Logon | Should be | Not Defined | Domain Controllers |
|   | 121 | Secure Socket Tunneling Protocol Service | Must be | Disabled | Domain Controllers |
|   | 122 | Security Accounts Manager | Must be | Automatic | Domain Controllers |
|   | 123 | Server | Should be | Not Defined | Domain Controllers |
|   | 124 | Server For Nfs | Must be | Disabled | Domain Controllers |
|   | 125 | Server For Nis | Must be | Disabled | Domain Controllers |
|   | 126 | Shell Hardware Detection | Must be | Automatic | Domain Controllers |
|   | 127 | Simple Mail Transport Protocol (smtp) | Must be | Disabled | Domain Controllers |
|   | 128 | Simple Tcp/ip Services | Must be | Disabled | Domain Controllers |
|   | 129 | Smart Card | Should be | Not Defined | Domain Controllers |
|   | 130 | Smart Card Removal Policy | Should be | Not Defined | Domain Controllers |
|   | 131 | Smb Hash Generation Service | Should be | Not Defined | Domain Controllers |
|   | 132 | Snmp Service | Should be | Not Defined | Domain Controllers |
|   | 133 | Snmp Trap | Should be | Not Defined | Domain Controllers |
|   | 134 | Software Protection | Should be | Not Defined | Domain Controllers |
|   | 135 | Special Administration Console Helper | Should be | Not Defined | Domain Controllers |
|   | 136 | Spp Notification Service | Should be | Not Defined | Domain Controllers |
|   | 137 | Sql Server Vss Writer | Should be | Not Defined | Domain Controllers |
|   | 138 | Ssdp Discovery | Must be | Disabled | Domain Controllers |
|   | 139 | Superfetch | Should be | Not Defined | Domain Controllers |
|   | 140 | System Event Notification Service | Should be | Not Defined | Domain Controllers |
|   | 141 | Task Scheduler | Must be | Automatic | Domain Controllers |
|   | 142 | Tcp/ip Netbios Helper | Must be | Automatic | Domain Controllers |
|   | 143 | Telephony | Should be | Not Defined | Domain Controllers |
|   | 144 | Telnet | Must be | Disabled | Domain Controllers |
|   | 145 | Themes | Should be | Not Defined | Domain Controllers |
|   | 146 | Thread Ordering Server | Should be | Not Defined | Domain Controllers |
|   | 147 | Tpm Base Services | Should be | Not Defined | Domain Controllers |
|   | 148 | Upnp Device Host | Must be | Disabled | Domain Controllers |
|   | 149 | User Profile Service | Must be | Automatic | Domain Controllers |
|   | 150 | Virtual Disk | Should be | Not Defined | Domain Controllers |
|   | 151 | Volume Shadow Copy | Should be | Not Defined | Domain Controllers |
|   | 152 | Web Management Service | Should be | Not Defined | Domain Controllers |
|   | 153 | Webclient | Should be | Not Defined | Domain Controllers |
|   | 154 | Windows Audio | Should be | Not Defined | Domain Controllers |
|   | 155 | Windows Audio Endpoint Builder | Should be | Not Defined | Domain Controllers |
|   | 156 | Windows Biometric Service | Should be | Not Defined | Domain Controllers |
|   | 157 | Windows Cardspace | Should be | Not Defined | Domain Controllers |
|   | 158 | Windows Color System | Should be | Not Defined | Domain Controllers |
|   | 159 | Windows Connect Now - Config Registrar | Must be | Disabled | Domain Controllers |
|   | 160 | Windows Defender | Should be | Not Defined | Domain Controllers |
|   | 161 | Windows Deployment Services Server | Must be | Disabled | Domain Controllers |
|   | 162 | Windows Driver Foundation - User-mode Driver Framework | Should be | Not Defined | Domain Controllers |
|   | 163 | Windows Error Reporting Service | Should be | Not Defined | Domain Controllers |
|   | 164 | Windows Event Collector | Should be | Not Defined | Domain Controllers |
|   | 165 | Windows Event Log | Must be | Automatic | Domain Controllers |
|   | 166 | Windows Firewall | Must be | Automatic | Domain Controllers |
|   | 167 | Windows Font Cache Service | Should be | Not Defined | Domain Controllers |
|   | 168 | Windows Image Acquisition (wia) | Should be | Not Defined | Domain Controllers |
|   | 169 | Windows Installer | Should be | Not Defined | Domain Controllers |
|   | 170 | Windows Internal Database (microsoft\*\*ssee) | Should be | Not Defined | Domain Controllers |
|   | 171 | Windows Internet Name Service (wins) | Must be | Disabled | Domain Controllers |
|   | 172 | Windows Management Instrumentation | Must be | Automatic | Domain Controllers |
|   | 173 | Windows Modules Installer | Should be | Not Defined | Domain Controllers |
|   | 174 | Windows Presentation Foundation Font Cache 3.0.0.0 | Should be | Not Defined | Domain Controllers |
|   | 175 | Windows Process Activation Service | Should be | Not Defined | Domain Controllers |
|   | 176 | Windows Remote Management (ws-management) | Should be | Not Defined | Domain Controllers |
|   | 177 | Windows Search | Should be | Not Defined | Domain Controllers |
|   | 178 | Windows System Resource Manager | Should be | Not Defined | Domain Controllers |
|   | 179 | Windows Time | Must be | Automatic | Domain Controllers |
|   | 180 | Windows Update | Must be | Automatic | Domain Controllers |
|   | 181 | Winhttp Web Proxy Auto-discovery Service | Should be | Not Defined | Domain Controllers |
|   | 182 | Wired Autoconfig | Must be | Automatic | Domain Controllers |
|   | 183 | Wlan Autoconfig | Must be | Disabled | Domain Controllers |
|   | 184 | Wmi Performance Adapter | Should be | Not Defined | Domain Controllers |
|   | 185 | Workstation | Must be | Automatic | Domain Controllers |
|   | 186 | World Wide Web Publishing Service | Must be | Disabled | Domain Controllers |

# 3.0 Windows Firewall Properties

## 3.1 Windows Firewall Properties\Domain Profile Tab

|  |  |
| --- | --- |
| **1.1.2.4.9.1.1** | **Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile Tab** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Windows Firewall: Domain: Apply Local Connection Security Rules | Should be | Not Configured | Domain Controllers |
|   | 2 | Windows Firewall: Domain: Apply Local Firewall Rules | Should be | Not Configured | Domain Controllers |
|   | 3 | Windows Firewall: Domain: Display A Notification | Should be | Not Configured | Domain Controllers |
|   | 4 | Windows Firewall: Domain: Firewall State | Should be | Not Configured | Domain Controllers |
|   | 5 | Windows Firewall: Domain: Inbound Connections | Should be | Not Configured | Domain Controllers |
|   | 6 | Windows Firewall: Domain: Outbound Connections | Should be | Not Configured | Domain Controllers |
|   | 7 | Windows Firewall: Domain: Allow Unicast Response | Should be | Not Configured | Domain Controllers |

## 3.2 Windows Firewall Properties\Private Profile Tab

|  |  |
| --- | --- |
| **1.1.2.4.9.1.2** | **Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile Tab** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Windows Firewall: Private: Allow Unicast Response | Should be | Not Configured | Domain Controllers |
|   | 2 | Windows Firewall: Private: Apply Local Connection Security Rules | Should be | Not Configured | Domain Controllers |
|   | 3 | Windows Firewall: Private: Apply Local Firewall Rules | Should be | Not Configured | Domain Controllers |
|   | 4 | Windows Firewall: Private: Display A Notification | Should be | Not Configured | Domain Controllers |
|   | 5 | Windows Firewall: Private: Firewall State | Should be | Not Configured | Domain Controllers |
|   | 6 | Windows Firewall: Private: Inbound Connections | Should be | Not Configured | Domain Controllers |
|   | 7 | Windows Firewall: Private: Outbound Connections | Should be | Not Configured | Domain Controllers |

## 3.3 Windows Firewall Properties\Public Profile Tab

|  |  |
| --- | --- |
| **1.1.2.4.9.1.3** | **Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile Tab** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Windows Firewall: Public: Allow Unicast Response | Should be | Not Configured | Domain Controllers |
|   | 2 | Windows Firewall: Public: Apply Local Connection Security Rules | Should be | Not Configured | Domain Controllers |
|   | 3 | Windows Firewall: Public: Apply Local Firewall Rules | Should be | Not Configured | Domain Controllers |
|   | 4 | Windows Firewall: Public: Display A Notification | Should be | Not Configured | Domain Controllers |
|   | 5 | Windows Firewall: Public: Firewall State | Should be | Not Configured | Domain Controllers |
|   | 6 | Windows Firewall: Public: Inbound Connections | Should be | Not Configured | Domain Controllers |
|   | 7 | Windows Firewall: Public: Outbound Connections | Should be | Not Configured | Domain Controllers |

# 4.0 Advanced Audit Policy Configuration

## 4.1 Advanced Audit Policy Configuration\Audit Policy\Account Logon

|  |  |
| --- | --- |
| **1.1.2.5.1** | **Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policy\Account Logon** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Audit Policy: Account Logon: Credential Validation | Must be | Success And Failure | Domain Controllers |
|   | 2 | Audit Policy: Account Logon: Kerberos Authentication Service | Should be | Not Configured | Domain Controllers |
|   | 3 | Audit Policy: Account Logon: Kerberos Service Ticket Operations | Should be | Not Configured | Domain Controllers |
|   | 4 | Audit Policy: Account Logon: Other Account Logon Events | Should be | Not Configured | Domain Controllers |

## 4.2 Advanced Audit Policy Configuration\Audit Policy\Account Management

|  |  |
| --- | --- |
| **1.1.2.5.2** | **Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policy\Account Management** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Audit Policy: Account Management: Application Group Management | Should be | Not Configured | Domain Controllers |
|   | 2 | Audit Policy: Account Management: Computer Account Management | Must be | Success And Failure | Domain Controllers |
|   | 3 | Audit Policy: Account Management: Distribution Group Management | Should be | Not Configured | Domain Controllers |
|   | 4 | Audit Policy: Account Management: Other Account Management Events | Must be | Success And Failure | Domain Controllers |
|   | 5 | Audit Policy: Account Management: Security Group Management | Must be | Success And Failure | Domain Controllers |
|   | 6 | Audit Policy: Account Management: User Account Management | Must be | Success And Failure | Domain Controllers |

## 4.3 Advanced Audit Policy Configuration\Audit Policy\Detailed Tracking

|  |  |
| --- | --- |
| **1.1.2.5.3** | **Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policy\Detailed Tracking** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Audit Policy: Detailed Tracking: Dpapi Activity | Must be | Success And Failure | Domain Controllers |
|   | 2 | Audit Policy: Detailed Tracking: Process Creation | Must be | Success | Domain Controllers |
|   | 3 | Audit Policy: Detailed Tracking: Process Termination | Should be | Not Configured | Domain Controllers |
|   | 4 | Audit Policy: Detailed Tracking: Rpc Events | Should be | Not Configured | Domain Controllers |

## 4.4 Advanced Audit Policy Configuration\Audit Policy\DS Access

|  |  |
| --- | --- |
| **1.1.2.5.4** | **Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policy\DS Access** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Audit Policy: Ds Access: Detailed Directory Service Replication | Must be | No Auditing | Domain Controllers |
|   | 2 | Audit Policy: Ds Access: Directory Service Access | Must be | Success And Failure | Domain Controllers |
|   | 3 | Audit Policy: Ds Access: Directory Service Changes | Must be | Success And Failure | Domain Controllers |
|   | 4 | Audit Policy: Ds Access: Directory Service Replication | Must be | No Auditing | Domain Controllers |

## 4.5 Advanced Audit Policy Configuration\Audit Policy\Logon Logoff

|  |  |
| --- | --- |
| **1.1.2.5.5** | **Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policy\Logon Logoff** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Audit Policy: Logon-logoff: Account Lockout | Must be | Success And Failure | Domain Controllers |
|   | 2 | Audit Policy: Logon-logoff: Ipsec Extended Mode | Should be | Not Configured | Domain Controllers |
|   | 3 | Audit Policy: Logon-logoff: Ipsec Main Mode | Should be | Not Configured | Domain Controllers |
|   | 4 | Audit Policy: Logon-logoff: Ipsec Quick Mode | Should be | Not Configured | Domain Controllers |
|   | 5 | Audit Policy: Logon-logoff: Logoff | Must be | Success | Domain Controllers |
|   | 6 | Audit Policy: Logon-logoff: Logon | Must be | Success And Failure | Domain Controllers |
|   | 7 | Audit Policy: Logon-logoff: Network Policy Server | Must be | Success And Failure | Domain Controllers |
|   | 8 | Audit Policy: Logon-logoff: Other Logon/logoff Events | Must be | Success And Failure | Domain Controllers |
|   | 9 | Audit Policy: Logon-logoff: Special Logon | Must be | Success | Domain Controllers |

## 4.6 Advanced Audit Policy Configuration\Audit Policy\Object Access

|  |  |
| --- | --- |
| **1.1.2.5.6** | **Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policy\Object Access** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Audit Policy: Object Access: application Generated | Should be | Not Configured | Domain Controllers |
|   | 2 | Audit Policy: Object Access: certification Services | Should be | Not Configured | Domain Controllers |
|   | 3 | Audit Policy: Object Access: detailed File Share | Should be | Not Configured | Domain Controllers |
|   | 4 | Audit Policy: Object Access: file Share | Must be | Success And Failure | Domain Controllers |
|   | 5 | Audit Policy: Object Access: file System | Must be | Success And Failure | Domain Controllers |
|   | 6 | Audit Policy: Object Access: filtering Platform Connection | Should be | Not Configured | Domain Controllers |
|   | 7 | Audit Policy: Object Access: filtering Platform Packet Drop | Should be | Not Configured | Domain Controllers |
|   | 8 | Audit Policy: Object Access: handle Manipulation | Must be | Success And Failure | Domain Controllers |
|   | 9 | Audit Policy: Object Access: kernel Object | Should be | Not Configured | Domain Controllers |
|   | 10 | Audit Policy: Object Access: other Object Access Events | Should be | Not Configured | Domain Controllers |
|   | 11 | Audit Policy: Object Access: registry | Must be | Success And Failure | Domain Controllers |
|   | 12 | Audit Policy: Object Access: sam | Should be | Not Configured | Domain Controllers |

## 4.7 Advanced Audit Policy Configuration\Audit Policy\Policy Change

|  |  |
| --- | --- |
| **1.1.2.5.7** | **Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policy\Policy Change** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Audit Policy: Policy Change: Audit Policy Change | Must be | Success And Failure | Domain Controllers |
|   | 2 | Audit Policy: Policy Change: Authentication Policy Change | Must be | Success | Domain Controllers |
|   | 3 | Audit Policy: Policy Change: Authorization Policy Change | Must be | Success | Domain Controllers |
|   | 4 | Audit Policy: Policy Change: Filtering Platform Policy Change | Should be | Not Configured | Domain Controllers |
|   | 5 | Audit Policy: Policy Change: Mpssvc Rule-level Policy Change | Should be | Not Configured | Domain Controllers |
|   | 6 | Audit Policy: Policy Change: Other Policy Change Events | Should be | Not Configured | Domain Controllers |

## 4.8 Advanced Audit Policy Configuration\Audit Policy\Privilege Use

|  |  |
| --- | --- |
| **1.1.2.5.8** | **Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policy\Privilege Use** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Audit Policy: Privilege Use: Non Sensitive Privilege Use | Should be | Not Configured | Domain Controllers |
|   | 2 | Audit Policy: Privilege Use: Other Privilege Use Events | Should be | Not Configured | Domain Controllers |
|   | 3 | Audit Policy: Privilege Use: Sensitive Privilege Use | Must be | Success And Failure | Domain Controllers |

## 4.9 Advanced Audit Policy Configuration\Audit Policy\Global Object Access Auditing

|  |  |
| --- | --- |
| **1.1.2.5.10** | **Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policy\Global Object Access Auditing** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Audit Policy: Global Object Access Auditing: File System | Must be | Failure: Everyone | Domain Controllers |
|   | 2 | Audit Policy: Global Object Access Auditing: Registry | Should be | Not Configured | Domain Controllers |

## 4.10 Advanced Audit Policy Configuration\Audit Policy\System

|  |  |
| --- | --- |
| **1.1.2.5.9** | **Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policy\System** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Audit Policy: System: Ipsec Driver | Must be | Success and Failure | Domain Controllers |
|   | 2 | Audit Policy: System: Other System Events | Must be | Success and Failure | Domain Controllers |
|   | 3 | Audit Policy: System: Security State Change | Must be | Success and Failure | Domain Controllers |
|   | 4 | Audit Policy: System: Security System Extension | Must be | Success and Failure | Domain Controllers |
|   | 5 | Audit Policy: System: System Integrity | Must be | Success and Failure | Domain Controllers |

# 5.0 Network

## 5.1 Network\Windows Connect Now

|  |  |
| --- | --- |
| **1.1.3.2.14** | **Computer Configuration\Policies\Administrative Templates\Network\Windows Connect Now** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Configuration Of Wireless Settings Using Windows Connect Now | Must be | Disabled | Domain Controllers |
|   | 2 | Prohibit Access Of The Windows Connect Now Wizards | Must be | Enabled | Domain Controllers |

## 5.2 Network\Link-Layer Topology Discovery

|  |  |
| --- | --- |
| **1.1.3.2.5** | **Computer Configuration\Policies\Administrative Templates\Network\Link-Layer Topology Discovery** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Turn On Mapper I/o (lltdio) Driver | Must be | Disabled | Domain Controllers |
|   | 2 | Turn On Responder (rspndr) Driver | Must be | Disabled | Domain Controllers |

## 5.3 Network\Microsoft Peer-to-Peer Networking Services

|  |  |
| --- | --- |
| **1.1.3.2.6** | **Computer Configuration\Policies\Administrative Templates\Network\Microsoft Peer-to-Peer Networking Services** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Turn Off Microsoft Peer-to-peer Networking Services | Must be | Enabled | Domain Controllers |

## 5.4 Network\Network Connections

|  |  |
| --- | --- |
| **1.1.3.2.7** | **Computer Configuration\Policies\Administrative Templates\Network\Network Connections** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Prohibit Installation And Configuration Of Network Bridge On Your Dns Domain Network | Must be | Enabled | Domain Controllers |
|   | 2 | Prohibit Use Of Internet Connection Sharing On Your Dns Domain Network | Must be | Enabled | Domain Controllers |

## 5.5 Network\Network Connections\Windows Firewall \Domain Profile

|  |  |
| --- | --- |
| **1.1.3.2.8.1.1** | **Computer Configuration\Policies\Administrative Templates\Network\Network Connections\Windows Firewall \Domain Profile** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Windows Firewall: Allow Icmp Exceptions | Should be | Not Configured | Domain Controllers |
|   | 2 | Windows Firewall: Allow Inbound File And Printer Sharing Exception | Should be | Not Configured | Domain Controllers |
|   | 3 | Windows Firewall: Allow Inbound Remote Administration Exception | Should be | Not Configured | Domain Controllers |
|   | 4 | Windows Firewall: Allow Inbound Remote Desktop Exceptions | Should be | Not Configured | Domain Controllers |
|   | 5 | Windows Firewall: Allow Inbound Upnp Framework Exceptions | Should be | Not Configured | Domain Controllers |
|   | 6 | Windows Firewall: Allow Local Port Exceptions | Should be | Not Configured | Domain Controllers |
|   | 7 | Windows Firewall: Allow Local Program Exceptions | Should be | Not Configured | Domain Controllers |
|   | 8 | Windows Firewall: Define Inbound Port Exceptions | Should be | Not Configured | Domain Controllers |
|   | 9 | Windows Firewall: Define Inbound Program Exceptions | Should be | Not Configured | Domain Controllers |
|   | 10 | Windows Firewall: Do Not Allow Exceptions | Should be | Not Configured | Domain Controllers |
|   | 11 | Windows Firewall: Prohibit Notifications | Should be | Not Configured | Domain Controllers |
|   | 12 | Windows Firewall: Prohibit Unicast Response To Multicast Or Broadcast Requests | Should be | Not Configured | Domain Controllers |
|   | 13 | Windows Firewall: Protect All Network Connections | Should be | Not Configured | Domain Controllers |

## 5.6 Network\Network Connections\Windows Firewall \Standard Profile

|  |  |
| --- | --- |
| **1.1.3.2.8.1.2** | **Computer Configuration\Policies\Administrative Templates\Network\Network Connections\Windows Firewall \Standard Profile** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Windows Firewall: Allow Icmp Exceptions | Should be | Not Configured | Domain Controllers |
|   | 2 | Windows Firewall: Allow Inbound File And Printer Sharing Exception | Should be | Not Configured | Domain Controllers |
|   | 3 | Windows Firewall: Allow Inbound Remote Administration Exception | Should be | Not Configured | Domain Controllers |
|   | 4 | Windows Firewall: Allow Inbound Remote Desktop Exceptions | Should be | Not Configured | Domain Controllers |
|   | 5 | Windows Firewall: Allow Inbound Upnp Framework Exceptions | Should be | Not Configured | Domain Controllers |
|   | 6 | Windows Firewall: Allow Local Port Exceptions | Should be | Not Configured | Domain Controllers |
|   | 7 | Windows Firewall: Allow Local Program Exceptions | Should be | Not Configured | Domain Controllers |
|   | 8 | Windows Firewall: Define Inbound Port Exceptions | Should be | Not Configured | Domain Controllers |
|   | 9 | Windows Firewall: Define Inbound Program Exceptions | Should be | Not Configured | Domain Controllers |
|   | 10 | Windows Firewall: Do Not Allow Exceptions | Should be | Not Configured | Domain Controllers |
|   | 11 | Windows Firewall: Prohibit Notifications | Should be | Not Configured | Domain Controllers |
|   | 12 | Windows Firewall: Prohibit Unicast Response To Multicast Or Broadcast Requests | Should be | Not Configured | Domain Controllers |
|   | 13 | Windows Firewall: Protect All Network Connections | Should be | Not Configured | Domain Controllers |

# 6.0 System

## 6.1 System\Group Policy

|  |  |
| --- | --- |
| **1.1.3.4.10** | **Computer Configuration\Policies\Administrative Templates\System\Group Policy** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Registry Policy Processing | Must be | Enabled: Process Even If The Group Policy Objects Have Not Changed | Domain Controllers |
|   | 2 | Turn Off Background Refresh Of Group Policy | Must be | Disabled | Domain Controllers |

## 6.2 System\Internet Communication Management\Internet Communication settings

|  |  |
| --- | --- |
| **1.1.3.4.11.1** | **Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Turn Off Automatic Root Certificates Update | Must be | Enabled | Domain Controllers |
|   | 2 | Turn Off Downloading Of Print Drivers Over Http | Must be | Enabled | Domain Controllers |
|   | 3 | Turn Off Event Viewer "events.asp" Links | Must be | Enabled | Domain Controllers |
|   | 4 | Turn Off Handwriting Recognition Error Reporting | Must be | Enabled | Domain Controllers |
|   | 5 | Turn Off Internet Connection Wizard If Url Connection Is Referring To Microsoft.com | Must be | Enabled | Domain Controllers |
|   | 6 | Turn Off Internet Download For Web Publishing And Online Ordering Wizards | Must be | Enabled | Domain Controllers |
|   | 7 | Turn Off Internet File Association Service | Must be | Enabled | Domain Controllers |
|   | 8 | Turn Off Printing Over Http | Must be | Enabled | Domain Controllers |
|   | 9 | Turn Off Registration If Url Connection Is Referring To Microsoft.com | Must be | Enabled | Domain Controllers |
|   | 10 | Turn Off Search Companion Content File Updates | Must be | Enabled | Domain Controllers |
|   | 11 | Turn Off The "publish To Web" Task For Files And Folders | Must be | Enabled | Domain Controllers |
|   | 12 | Turn Off The "order Prints" Picture Task | Must be | Enabled | Domain Controllers |
|   | 13 | Turn Off The Windows Messenger Customer Experience Improvement Program | Must be | Enabled | Domain Controllers |
|   | 14 | Turn Off Windows Customer Experience Improvement Program | Must be | Enabled | Domain Controllers |
|   | 15 | Turn Off Windows Error Reporting | Must be | Enabled | Domain Controllers |
|   | 16 | Turn Off Windows Update Device Driver Searching | Must be | Enabled | Domain Controllers |

## 6.3 System\Logon

|  |  |
| --- | --- |
| **1.1.3.4.16** | **Computer Configuration\Policies\Administrative Templates\System\Logon** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Always Use Classic Logon | Must be | Enabled | Domain Controllers |
|   | 2 | Do Not Process The Legacy Run List | Should be | Not Configured | Domain Controllers |
|   | 3 | Do Not Process The Run Once List | Should be | Not Configured | Domain Controllers |
|   | 4 | Hide Entry Points For Fast User Switching | Must be | Enabled | Domain Controllers |

## 6.4 System\Power Management\Sleep Settings

|  |  |
| --- | --- |
| **1.1.3.4.19.4** | **Computer Configuration\Policies\Administrative Templates\System\Power Management\Sleep Settings** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Require A Password When A Computer Wakes (on Battery) | Must be | Enabled | Domain Controllers |
|   | 2 | Require A Password When A Computer Wakes (plugged In) | Must be | Enabled | Domain Controllers |

## 6.5 System\Remote Assistance

|  |  |
| --- | --- |
| **1.1.3.4.21** | **Computer Configuration\Policies\Administrative Templates\System\Remote Assistance** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Offer Remote Assistance | Must be | Disabled | Domain Controllers |
|   | 2 | Solicited Remote Assistance | Must be | Disabled | Domain Controllers |
|   | 3 | Turn On Session Logging | Must be | Enabled | Domain Controllers |

## 6.6 System\Remote Procedure Call

|  |  |
| --- | --- |
| **1.1.3.4.22** | **Computer Configuration\Policies\Administrative Templates\System\Remote Procedure Call** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Restrictions For Unauthenticated Rpc Clients | Should be | Not Configured | Domain Controllers |
|   | 2 | Rpc Endpoint Mapper Client Authentication | Should be | Not Configured | Domain Controllers |

## 6.7 System\Windows Time Service\Time Providers

|  |  |
| --- | --- |
| **1.1.3.4.33** | **Computer Configuration\Policies\Administrative Templates\System\Windows Time Service\Time Providers** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Configure Windows Ntp Client | Should be | Not Configured | Domain Controllers |

## 6.8 System\Driver Installation

|  |  |
| --- | --- |
| **1.1.3.4.7** | **Computer Configuration\Policies\Administrative Templates\System\Driver Installation** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Turn Off Windows Update Device Driver Search Prompt | Must be | Enabled | Domain Controllers |

# 7.0 Event Log Service

## 7.1 Event Log Service\Application

|  |  |
| --- | --- |
| **1.1.3.5.13.1** | **Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\Application** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Maximum Log Size (kb) | Must be | 102400 | Domain Controllers |
|   | 2 | Retain Old Events | Must be | Disabled | Domain Controllers |

## 7.2 Event Log Service\Security

|  |  |
| --- | --- |
| **1.1.3.5.13.2** | **Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\Security** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Maximum Log Size (kb) | Must be | 409600 | Domain Controllers |
|   | 2 | Retain Old Events | Must be | Disabled | Domain Controllers |

## 7.3 Event Log Service\System

|  |  |
| --- | --- |
| **1.1.3.5.13.4** | **Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\System** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Maximum Log Size (kb) | Must be | 102400 | Domain Controllers |
|   | 2 | Retain Old Events | Must be | Disabled | Domain Controllers |

# 8.0 Internet Explorer

## 8.1 Internet Explorer

|  |  |
| --- | --- |
| **1.1.3.5.17** | **Computer Configuration\Policies\Administrative Templates\Windows Components\Internet Explorer** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Disable Automatic Install Of Internet Explorer Components | Should be | Not Configured | Domain Controllers |
|   | 2 | Disable Periodic Check For Internet Explorer Software Updates | Must be | Enabled | Domain Controllers |
|   | 3 | Disable Software Update Shell Notifications On Program Launch | Should be | Not Configured | Domain Controllers |
|   | 4 | Do Not Allow Users To Enable Or Disable Add-ons | Should be | Not Configured | Domain Controllers |
|   | 5 | Make Proxy Settings Per-machine (rather Than Per-user) | Should be | Not Configured | Domain Controllers |
|   | 6 | Security Zones: Do Not Allow Users To Add/delete Sites | Should be | Not Configured | Domain Controllers |
|   | 7 | Security Zones: Do Not Allow Users To Change Policies | Should be | Not Configured | Domain Controllers |
|   | 8 | Security Zones: Use Only Machine Settings | Should be | Not Configured | Domain Controllers |
|   | 9 | Turn Off Crash Detection | Should be | Not Configured | Domain Controllers |

## 8.2 Internet Explorer\Internet Control Panel\Advanced Page

|  |  |
| --- | --- |
| **1.1.3.5.17.7** | **Computer Configuration\Policies\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Advanced Page** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Allow Software To Run Or Install Even If The Signature Is Invalid | Should be | Not Configured | Domain Controllers |

## 8.3 Internet Explorer\Security Features\Add-on Management

|  |  |
| --- | --- |
| **1.1.3.5.17.9.1** | **Computer Configuration\Policies\Administrative Templates\Windows Components\Internet Explorer\Security Features\Add-on Management** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Add-on List | Should be | Not Configured | Domain Controllers |
|   | 2 | Deny All Add-ons Unless Specifically Allowed In The Add-on List | Should be | Not Configured | Domain Controllers |

## 8.4 Internet Explorer\Security Features\Protection from Zone Elevation

|  |  |
| --- | --- |
| **1.1.3.5.17.9.11** | **Computer Configuration\Policies\Administrative Templates\Windows Components\Internet Explorer\Security Features\Protection From Zone Elevation** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Internet Explorer Processes | Should be | Not Configured | Domain Controllers |

## 8.5 Internet Explorer\Security Features\Restrict ActiveX Install

|  |  |
| --- | --- |
| **1.1.3.5.17.9.12** | **Computer Configuration\Policies\Administrative Templates\Windows Components\Internet Explorer\Security Features\Restrict ActiveX Install** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Internet Explorer Processes | Should be | Not Configured | Domain Controllers |

## 8.6 Internet Explorer\Security Features\Restrict File Download

|  |  |
| --- | --- |
| **1.1.3.5.17.9.13** | **Computer Configuration\Policies\Administrative Templates\Windows Components\Internet Explorer\Security Features\Restrict File Download** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Internet Explorer Processes | Should be | Not Configured | Domain Controllers |

## 8.7 Internet Explorer\Security Features\Scripted Window Security Restrictions

|  |  |
| --- | --- |
| **1.1.3.5.17.9.14** | **Computer Configuration\Policies\Administrative Templates\Windows Components\Internet Explorer\Security Features\Scripted Window Security Restrictions** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Internet Explorer Processes | Should be | Not Configured | Domain Controllers |

## 8.8 Internet Explorer\Security Features\Consistent Mime Handling

|  |  |
| --- | --- |
| **1.1.3.5.17.9.4** | **Computer Configuration\Policies\Administrative Templates\Windows Components\Internet Explorer\Security Features\Consistent Mime Handling** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Internet Explorer Processes | Should be | Not Configured | Domain Controllers |

## 8.9 Internet Explorer\Security Features\Mime Sniffing Safety Feature

|  |  |
| --- | --- |
| **1.1.3.5.17.9.7** | **Computer Configuration\Policies\Administrative Templates\Windows Components\Internet Explorer\Security Features\Mime Sniffing Safety Feature** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Internet Explorer Processes | Should be | Not Configured | Domain Controllers |

## 8.10 Internet Explorer\Security Features\MK Protocol Security Restriction

|  |  |
| --- | --- |
| **1.1.3.5.17.9.8** | **Computer Configuration\Policies\Administrative Templates\Windows Components\Internet Explorer\Security Features\MK Protocol Security Restriction** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Internet Explorer Processes | Should be | Not Configured | Domain Controllers |

# 9.0 Windows Components

## 9.1 Windows Components\NetMeeting

|  |  |
| --- | --- |
| **1.1.3.5.20** | **Computer Configuration\Policies\Administrative Templates\Windows Components\NetMeeting** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Disable Remote Desktop Sharing | Must be | Enabled | Domain Controllers |

## 9.2 Windows Components\Online Assistance

|  |  |
| --- | --- |
| **1.1.3.5.23** | **Computer Configuration\Policies\Administrative Templates\Windows Components\Online Assistance** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Turn Off Active Help | Must be | Enabled | Domain Controllers |

## 9.3 Windows Components\Remote Desktop Services\Remote Desktop Connection Client

|  |  |
| --- | --- |
| **1.1.3.5.27.2** | **Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Connection Client** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Do Not Allow Passwords To Be Saved | Must be | Enabled | Domain Controllers |

## 9.4 Windows Components\Remote Desktop Services\Remote Desktop Session Host\Session Time Limits

|  |  |
| --- | --- |
| **1.1.3.5.27.3.10** | **Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Session Time Limits** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Set Time Limit For Disconnected Sessions | Should be | Not Configured | Domain Controllers |
|   | 2 | Set Time Limit For Active But Idle Terminal Services Sessions | Should be | Not Configured | Domain Controllers |
|   | 3 | Set Time Limit For Active But Idle Terminal Services Sessions | Should be | Not Configured | Domain Controllers |
|   | 4 | Set Time Limit For Disconnected Sessions | Should be | Not Configured | Domain Controllers |

## 9.5 Windows Components\Remote Desktop Services\Remote Desktop Session Host\Temporary folders

|  |  |
| --- | --- |
| **1.1.3.5.27.3.11** | **Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Temporary folders** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Do Not Delete Temp Folder Upon Exit | Should be | Not Configured | Domain Controllers |
|   | 2 | Do Not Use Temp Folders Per Session | Should be | Not Configured | Domain Controllers |

## 9.6 Windows Components\Remote Desktop Services\Remote Desktop Session Host\Connections

|  |  |
| --- | --- |
| **1.1.3.5.27.3.2** | **Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Connections** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Allow Users To Connect Remotely Using Remote Desktop Services | Should be | Not Configured | Domain Controllers |
|   | 2 | Set Rules For Remote Control Of Remote Desktop Services User Sessions | Must be | Enabled: Full Control With User's Permissions | Domain Controllers |
|   | 3 | Restrict Users To A Single Remote Remote Desktop Services Session | Should be | Not Configured | Domain Controllers |

## 9.7 Windows Components\Remote Desktop Services\Remote Desktop Session Host\Device and Resource Redirection

|  |  |
| --- | --- |
| **1.1.3.5.27.3.3** | **Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Device and Resource Redirection** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Allow Audio And Video Playback Redirection | Must be | Disabled | Domain Controllers |
|   | 2 | Allow Audio Recording Redirection | Must be | Disabled | Domain Controllers |
|   | 3 | Allow Time Zone Redirection | Should be | Not Configured | Domain Controllers |
|   | 4 | Do Not Allow Clipboard Redirection | Should be | Not Configured | Domain Controllers |
|   | 5 | Do Not Allow Com Port Redirection | Must be | Enabled | Domain Controllers |
|   | 6 | Do Not Allow Drive Redirection | Must be | Enabled | Domain Controllers |
|   | 7 | Do Not Allow Lpt Port Redirection | Must be | Enabled | Domain Controllers |
|   | 8 | Do Not Allow Smart Card Device Redirection | Must be | Disabled | Domain Controllers |
|   | 9 | Do Not Allow Supported Plug And Play Device Redirection | Must be | Enabled | Domain Controllers |

## 9.8 Windows Components\Remote Desktop Services\Remote Desktop Session Host\Printer Redirection

|  |  |
| --- | --- |
| **1.1.3.5.27.3.5** | **Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Printer Redirection** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Do Not Allow Client Printer Redirection | Must be | Enabled | Domain Controllers |

## 9.9 Windows Components\Remote Desktop Services\Remote Desktop Session Host\Remote Session Environment

|  |  |
| --- | --- |
| **1.1.3.5.27.3.8** | **Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Remote Session Environment** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Remove "disconnect" Option From The Shut Down Dialog | Should be | Not Configured | Domain Controllers |

## 9.10 Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security

|  |  |
| --- | --- |
| **1.1.3.5.27.3.9** | **Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Always Prompt For Password Upon Connection | Must be | Enabled | Domain Controllers |
|   | 2 | Require Secure Rpc Communication | Must be | Enabled | Domain Controllers |
|   | 3 | Require User Authentication For Remote Connections By Using Network Level Authentication | Must be | Enabled | Domain Controllers |
|   | 4 | Set Client Connection Encryption Level | Must be | Enabled:high Level | Domain Controllers |

## 9.11 Windows Components\RSS Feeds

|  |  |
| --- | --- |
| **1.1.3.5.28** | **Computer Configuration\Policies\Administrative Templates\Windows Components\RSS Feeds** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Turn Off Downloading Of Enclosures | Must be | Enabled | Domain Controllers |

## 9.12 Windows Components\AutoPlay Policies

|  |  |
| --- | --- |
| **1.1.3.5.4** | **Computer Configuration\Policies\Administrative Templates\Windows Components\AutoPlay Policies** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Default Behavior For Autorun | Must be | Enabled: Do Not Execute Any Autorun Commands | Domain Controllers |
|   | 2 | Turn Off Autoplay | Must be | Enabled:all Drives | Domain Controllers |
|   | 3 | Turn Off Autoplay For Non-volume Devices | Must be | Enabled | Domain Controllers |

## 9.13 Windows Components\Windows Defender

|  |  |
| --- | --- |
| **1.1.3.5.40** | **Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Defender** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Configure Microsoft Spynet Reporting | Must be | Disabled | Domain Controllers |

## 9.14 Windows Components\Windows Error Reporting

|  |  |
| --- | --- |
| **1.1.3.5.41** | **Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Error Reporting** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Disable Logging | Must be | Disabled | Domain Controllers |
|   | 2 | Disable Windows Error Reporting | Must be | Enabled | Domain Controllers |
|   | 3 | Do Not Send Additional Data | Must be | Enabled | Domain Controllers |

## 9.15 Windows Components\Windows Explorer

|  |  |
| --- | --- |
| **1.1.3.5.42** | **Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Explorer** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Turn Off Heap Termination On Corruption | Should be | Not Configured | Domain Controllers |
|   | 2 | Turn Off Shell Protocol Protected Mode | Should be | Not Configured | Domain Controllers |

## 9.16 Windows Components\Windows Installer

|  |  |
| --- | --- |
| **1.1.3.5.43** | **Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Installer** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Allow Admin To Install From Terminal Services Session | Must be | Enabled | Domain Controllers |
|   | 2 | Disable Ie Security Prompt For Windows Installer Scripts | Should be | Not Configured | Domain Controllers |
|   | 3 | Enable User Control Over Installs | Should be | Not Configured | Domain Controllers |
|   | 4 | Logging | Must be | Enabled = Iweap (status Messages, Warnings, Errors, Start Up Actions, Terminal Properites) | Domain Controllers |
|   | 5 | Prohibit Non-administrators From Applying Vendor Signed Updates | Should be | Not Configured | Domain Controllers |

## 9.17 Windows Components\Windows Logon Options

|  |  |
| --- | --- |
| **1.1.3.5.44** | **Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Logon Options** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Report When Logon Server Was Not Available During User Logon | Must be | Enabled | Domain Controllers |

## 9.18 Windows Components\Windows Mail

|  |  |
| --- | --- |
| **1.1.3.5.45** | **Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Mail** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Turn Off The Communities Features | Must be | Enabled | Domain Controllers |
|   | 2 | Turn Off Windows Mail Application | Must be | Enabled | Domain Controllers |

## 9.19 Windows Components\Windows Media Digital Rights Management

|  |  |
| --- | --- |
| **1.1.3.5.47** | **Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Media Digital Rights Management** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Prevent Windows Media Drm Internet Access | Must be | Enabled | Domain Controllers |

## 9.20 Windows Components\Windows Media Player

|  |  |
| --- | --- |
| **1.1.3.5.48** | **Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Media Player** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Do Not Show First Use Dialog Boxes | Must be | Enabled | Domain Controllers |
|   | 2 | Prevent Automatic Updates | Must be | Enabled | Domain Controllers |

## 9.21 Windows Components\Windows Messenger

|  |  |
| --- | --- |
| **1.1.3.5.49** | **Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Messenger** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Do Not Allow Windows Messenger To Be Run | Must be | Enabled | Domain Controllers |
|   | 2 | Do Not Automatically Start Windows Messenger Initially | Must be | Enabled | Domain Controllers |

## 9.22 Windows Components\Windows PowerShell

|  |  |
| --- | --- |
| **1.1.3.5.51** | **Computer Configuration\Policies\Administrative Templates\Windows Components\Windows PowerShell** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Turn On Script Execution | Must be | Enabled: Allow Local Scripts And Remote Signed Scripts | Domain Controllers |

## 9.23 Windows Components\Windows Remote Management (WinRM)\WinRM Client

|  |  |
| --- | --- |
| **1.1.3.5.53.1** | **Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Client** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Allow Basic Authentication | Must be | Disabled | Domain Controllers |
|   | 2 | Allow Credssp Authentication | Must be | Disabled | Domain Controllers |
|   | 3 | Allow Unencrypted Traffic | Must be | Disabled | Domain Controllers |
|   | 4 | Disallow Digest Authentication | Must be | Disabled | Domain Controllers |
|   | 5 | Disallow Kerberos Authentication | Must be | Disabled | Domain Controllers |
|   | 6 | Disallow Negotiate Authentication | Must be | Disabled | Domain Controllers |
|   | 7 | Trusted Hosts | Must be | Disabled | Domain Controllers |

## 9.24 Windows Components\Windows Remote Management (WinRM)\WinRM Service

|  |  |
| --- | --- |
| **1.1.3.5.53.2** | **Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Service** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Allow Automatic Configuration Of Listeners (ipv4) | Should be | Not Configured | Domain Controllers |
|   | 2 | Allow Automatic Configuration Of Listeners (ipv6) | Should be | Not Configured | Domain Controllers |
|   | 3 | Allow Basic Authentication | Must be | Disabled | Domain Controllers |
|   | 4 | Allow Credssp Authentication | Must be | Disabled | Domain Controllers |
|   | 5 | Allow Unencrypted Traffic | Must be | Disabled | Domain Controllers |
|   | 6 | Disallow Kerberos Authentication | Must be | Disabled | Domain Controllers |
|   | 7 | Disallow Negotiate Authentication | Must be | Disabled | Domain Controllers |
|   | 8 | Specify Channel Binding Token Hardening Level | Must be | Enabled, Strict | Domain Controllers |
|   | 9 | Turn On Compatibility Http Listener | Should be | Not Configured | Domain Controllers |
|   | 10 | Turn On Compatibility Https Listener | Should be | Not Configured | Domain Controllers |

## 9.25 Windows Components\Windows Remote Shell

|  |  |
| --- | --- |
| **1.1.3.5.54** | **Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Shell** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Allow Remote Shell Access | Must be | Enabled | Domain Controllers |
|   | 2 | Maxconcurrentusers | Should be | Not Configured | Domain Controllers |
|   | 3 | Specify Idle Timeout | Should be | Not Configured | Domain Controllers |
|   | 4 | Specify Maximum Amount Of Memory In Mb Per Shell | Should be | Not Configured | Domain Controllers |
|   | 5 | Specify Maximum Number Of Processes Per Shell | Should be | Not Configured | Domain Controllers |
|   | 6 | Specify Maximum Number Of Remote Shells Per User | Should be | Not Configured | Domain Controllers |
|   | 7 | Specify Shell Timeout | Should be | Not Configured | Domain Controllers |

## 9.26 Windows Components\Windows Update

|  |  |
| --- | --- |
| **1.1.3.5.57** | **Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Update** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Configure Automatic Updates | Should be | Not Configured | Domain Controllers |
|   | 2 | Do Not Adjust Default Option To 'install Updates And Shut Down' In Shut Down Windows Dialog Box | Should be | Not Configured | Domain Controllers |
|   | 3 | Do Not Display 'install Updates And Shut Down' Option In Shut Down Windows Dialog Box | Should be | Not Configured | Domain Controllers |
|   | 4 | No Auto-restart With Logged On Users For Scheduled Automatic Updates Installations | Should be | Not Configured | Domain Controllers |
|   | 5 | Reschedule Automatic Updates Scheduled Installations | Should be | Not Configured | Domain Controllers |

## 9.27 Windows Components\Credential User Interface

|  |  |
| --- | --- |
| **1.1.3.5.8** | **Computer Configuration\Policies\Administrative Templates\Windows Components\Credential User Interface** |
|  | **Item** | **Setting** | **Compliance Level** | **Value** | **Applicability** |
|   | 1 | Enumerate Administrator Accounts On Elevation | Must be | Disabled | Domain Controllers |
|   | 2 | Require Trusted Path For Credential Entry | Should be | Not Configured | Domain Controllers |