Configure Automatic Updates	Enabled: - Auto download	Computer
	and notify for install.	Configuration
	5	ative
		Templates\Windows
		Components\Windows
		Update\Configure
		Automatic Updates
Minimum Password Length	8 Characters	Computer
ivininiani i uss vora Dongui		Configuration\Windows
		Settings/Security
		Settings Account
		Policies/Password
		Policy/Minimum
		nessword length
Maximum Decenvord Ago	60 David	Computer
Maximum Fassword Age	00 Days	Configuration\Windows
		Configuration/windows
		Settings/Security
		Settings\Account Dell'siss\Deserversel
		Policies Password
		password age
Minimum Password Age	1 day	
Password Complexity	Enabled	Computer
		Configuration\Windows
		Settings\Security
		Settings\Account
		Policies\Password
		Policy\Password must
		meet complexity
		requirements
Password History	24 passwords remembered	Computer
		Configuration\Windows
		Settings\Security
		Settings\Account
		Policies\Password
		Policy\Enforce password
		history
Store Passwords using	Disabled	Computer
Reversible Encryption		Configuration\Windows
		Settings\Security
		Settings\Account
		Policies
		Policy\Store passwords
		using reversible
		encryption
Account Lockout Duration	15 minutes	Computer
		Configuration\Windows
		Settings\Security
		Settings\Account
		Policies\Account
		1 Oncies/recount

		Lockout Policy\Account
		lockout duration
Account Lockout Threshold	3 attempts	Computer
	L.	Configuration\Windows
		Settings\Security
		Settings\Account
		Policies\Account
		Lockout Policy Account
		lockout threshold
Reset Account Lockout After	15 minutes	Computer
Rebet / Recount Lockout / Inter	10 millious	Configuration Windows
		Settings/Security
		Settings Account
		Policies
		Lockout Policy/Reset
		account lockout counter
		after
Enforce user logen restrictions	Enchlad	Computer
Enforce user logon restrictions	Enabled	Configuration Windows
		Sottings/Socurity
		Settings Security
		Delicies Kerberge
		Policy/Enforce year
Discoursest alignets where losses	Eachlad	Commuter
bourg auring	Enabled	Configuration Windows
nours expire		Configuration \windows
		Settings\Security
		Delicies Security
		Ontions/Microsoft
		notwork server:
		Disconnect clients when
		logon hours expire
Access Credential Manager of a	Set to 'No Ono'	Computer
trusted caller'		Configuration Windows
trusted callel		Sottings/Socurity
		Settings/Security
		Policies/User Rights
		Assignment/Access
		Credential Manager as a
		trusted caller
Set 'Access this computer from	Level 1 - Domain	Computer
the network'	Controller The	Configuration\Windows
	recommended state for this	Settings/Security
	setting is: Administrators	Settings/Security Settings/Local
	Authenticated Users	Policies/User Rights
	ENTERDISE DOMAIN	Assignment Access this
	CONTROLLERS	computer from the
	Level 1 - Member Server	network
	The recommended state	
	Authenticated Users, ENTERPRISE DOMAIN CONTROLLERS. Level 1 - Member Server. The recommended state	Assignment\Access this computer from the network

	for this setting is:	
	Administrators,	
	Authenticated Users.	
Set 'Act as part of the operating		Computer
system' to 'No One'		Configuration
		Settings/Security
		Settings/Local
		Policies\User Rights
		Assignment Act as part
		of the operating system
Set 'Add workstations to	Level 1 - Domain	Computer
domain' to 'Administrators'	Controller	Configuration Windows
domain to Administrators	Controller	Sottings/Socurity
		Settings/Legel
		Deligias/User Dishts
		Policies User Rights
		Assignment\Add
		workstations to domain
Set 'Adjust memory quotas for a	Level I - Domain	Computer
process' to 'Administrators,	Controller	Configuration/Windows
LOCAL SERVICE,	Level 1 - Member Server	Settings\Security
NETWORK SERVICE'		Settings\Local
		Policies\User Rights
		Assignment\Adjust
		memory quotas for a
		process
Set 'Allow log on locally' to	Level 1 - Domain	Computer
'Administrators'	Controller	Configuration\Windows
	Level 1 - Member Server	Settings\Security
		Settings\Local
		Policies\User Rights
		Assignment\Allow log
		on locally
Configure 'Allow log on	Domain controllers:	Computer
through Remote Desktop	Administrators.	Configuration
Services'	Member servers	Settings/Security
	Administrators, Remote	Settings/Local
	Desktop Users	Policies/User Rights
		Assignment/Allow log
		on through Remote
		Deskton Services
Set 'Back up files and	Level 1 - Domain	Computer
directories' to 'Administrators'		Configuration Windows
	Controller	
	Controller Level 1 - Member Server	Settings/Security
	Level 1 - Member Server	Settings\Local
	Level 1 - Member Server	Settings\Security Settings\Local Policies\Liser Pights
	Level 1 - Member Server	Settings\Security Settings\Local Policies\User Rights
	Level 1 - Member Server	Settings\Security Settings\Local Policies\User Rights Assignment\Back up
	Level 1 - Member Server	Settings\Security Settings\Local Policies\User Rights Assignment\Back up files and directories
Set 'Change the system time' to	Level 1 - Member Server	Settings\Security Settings\Local Policies\User Rights Assignment\Back up files and directories Computer
Set 'Change the system time' to 'Administrators, LOCAL	Level 1 - Member Server	Settings\Security Settings\Local Policies\User Rights Assignment\Back up files and directories Computer Configuration\Windows

		Settings\Local
		Policies\User Rights
		Assignment\Change the
		system time
Set 'Change the time zone' to	Level 1 - Domain	Computer
'Administrators, LOCAL	Controller	Configuration
SERVICE'	Level 1 - Member Server	Settings\Security
		Settings\Local
		Policies\User Rights
		Assignment/Change the
		time zone
Set 'Create a pagefile' to	Level 1 - Domain	Computer
'Administrators'	Controller	Configuration Windows
7 tunnistators	Level 1 - Member Server	Settings/Security
		Settings/Local
		Policies/User Rights
		Assignment/Create a
		Assignment/Create a
Sat 'Crasta a tokan abjact' to	Lavel 1 Domain	Computer
'No Opo'	Controllor	Configuration Windows
No Olle	Loval 1 Mambar Samuar	Configuration/windows
	Level 1 - Member Server	Settings/Security
		Settings\Local
		Policies\User Rights
		Assignment Create a
		token object
Set Create global objects to	Level I - Domain	Computer
Administrators, LOCAL	Controller	Configuration\Windows
SERVICE, NEIWORK	Level 1 - Member Server	Settings\Security
SERVICE, SERVICE		Settings\Local
		Policies\User Rights
		Assignment\Create
		global objects
Set 'Create permanent shared	Level 1 - Domain	global objects Computer
Set 'Create permanent shared objects' to 'No One'	Level 1 - Domain Controller	global objects Computer Configuration\Windows
Set 'Create permanent shared objects' to 'No One'	Level 1 - Domain Controller Level 1 - Member Server	global objects Computer Configuration\Windows Settings\Security
Set 'Create permanent shared objects' to 'No One'	Level 1 - Domain Controller Level 1 - Member Server	global objects Computer Configuration\Windows Settings\Security Settings\Local
Set 'Create permanent shared objects' to 'No One'	Level 1 - Domain Controller Level 1 - Member Server	global objects Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights
Set 'Create permanent shared objects' to 'No One'	Level 1 - Domain Controller Level 1 - Member Server	global objects Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Create
Set 'Create permanent shared objects' to 'No One'	Level 1 - Domain Controller Level 1 - Member Server	global objectsComputerConfiguration\WindowsSettings\SecuritySettings\LocalPolicies\User RightsAssignment\Createpermanent shared
Set 'Create permanent shared objects' to 'No One'	Level 1 - Domain Controller Level 1 - Member Server	global objectsComputerConfiguration\WindowsSettings\SecuritySettings\LocalPolicies\User RightsAssignment\Createpermanent sharedobjects
Set 'Create permanent shared objects' to 'No One' Set 'Create symbolic links' to	Level 1 - Domain Controller Level 1 - Member Server Level 1 - Domain	global objectsComputerConfiguration\WindowsSettings\SecuritySettings\LocalPolicies\User RightsAssignment\Createpermanent sharedobjectsComputer
Set 'Create permanent shared objects' to 'No One' Set 'Create symbolic links' to 'Administrators'	Level 1 - Domain Controller Level 1 - Member Server Level 1 - Domain Controller	global objectsComputerConfiguration\WindowsSettings\SecuritySettings\LocalPolicies\User RightsAssignment\Createpermanent sharedobjectsComputerConfiguration\Windows
Set 'Create permanent shared objects' to 'No One' Set 'Create symbolic links' to 'Administrators'	Level 1 - Domain Controller Level 1 - Member Server Level 1 - Domain Controller Level 1 - Member Server	global objectsComputerConfiguration\WindowsSettings\SecuritySettings\LocalPolicies\User RightsAssignment\Createpermanent sharedobjectsComputerConfiguration\WindowsSettings\Security
Set 'Create permanent shared objects' to 'No One' Set 'Create symbolic links' to 'Administrators'	Level 1 - Domain Controller Level 1 - Member Server Level 1 - Domain Controller Level 1 - Member Server	global objectsComputerConfiguration\WindowsSettings\SecuritySettings\LocalPolicies\User RightsAssignment\Createpermanent sharedobjectsComputerConfiguration\WindowsSettings\SecuritySettings\Local
Set 'Create permanent shared objects' to 'No One' Set 'Create symbolic links' to 'Administrators'	Level 1 - Domain Controller Level 1 - Member Server Level 1 - Domain Controller Level 1 - Member Server	global objectsComputerConfiguration\WindowsSettings\SecuritySettings\LocalPolicies\User RightsAssignment\Createpermanent sharedobjectsComputerConfiguration\WindowsSettings\SecuritySettings\LocalPolicies\User Rights
Set 'Create permanent shared objects' to 'No One' Set 'Create symbolic links' to 'Administrators'	Level 1 - Domain Controller Level 1 - Member Server Level 1 - Domain Controller Level 1 - Member Server	global objectsComputerConfiguration\WindowsSettings\SecuritySettings\LocalPolicies\User RightsAssignment\Createpermanent sharedobjectsComputerConfiguration\WindowsSettings\SecuritySettings\LocalPolicies\User RightsAssignment\Create
Set 'Create permanent shared objects' to 'No One' Set 'Create symbolic links' to 'Administrators'	Level 1 - Domain Controller Level 1 - Member Server Level 1 - Domain Controller Level 1 - Member Server	global objectsComputerConfiguration\WindowsSettings\SecuritySettings\LocalPolicies\User RightsAssignment\Createpermanent sharedobjectsComputerConfiguration\WindowsSettings\SecuritySettings\LocalPolicies\User RightsAssignment\Createsettings\SecuritySettings\LocalPolicies\User RightsAssignment\Createsymbolic links
Set 'Create permanent shared objects' to 'No One' Set 'Create symbolic links' to 'Administrators' Set 'Debug programs' to	Level 1 - Domain Controller Level 1 - Member Server Level 1 - Domain Controller Level 1 - Member Server	global objectsComputerConfiguration\WindowsSettings\SecuritySettings\LocalPolicies\User RightsAssignment\Createpermanent sharedobjectsComputerConfiguration\WindowsSettings\SecuritySettings\LocalPolicies\User RightsAssignment\Createsymbolic linksComputer
Set 'Create permanent shared objects' to 'No One' Set 'Create symbolic links' to 'Administrators' Set 'Debug programs' to 'Administrators'	Level 1 - Domain Controller Level 1 - Member Server Level 1 - Domain Controller Level 1 - Member Server Level 1 - Member Server	global objectsComputerConfiguration\WindowsSettings\SecuritySettings\LocalPolicies\User RightsAssignment\Createpermanent sharedobjectsComputerConfiguration\WindowsSettings\SecuritySettings\LocalPolicies\User RightsAssignment\Createsymbolic linksComputerComputerConfiguration\Windows

		Settings\Local
		Policies/User Rights
		Assignment\Debug
Set 'Deny access to this	Level 1 Domain	Computer
computer from the network'	Controller The	Configuration Windows
computer from the network	recommended state for this	Settings/Security
	setting is to include.	Settings\Local
	Guests Local account	Policies\User Rights
	Level 1 - Member Server	Assignment/Deny access
	The recommended state	to this computer from
	for this setting is to	the network
	include: Guests, Local	
	account and member of	
	Administrators group.	
Set 'Deny log on as a batch job'	Level 1 - Domain	Computer
to include 'Guests'	Controller	Configuration\Windows
	Level 1 - Member Server	Settings\Security
		Settings\Local
		Policies\User Rights
		Assignment\Deny log on
		as a batch job
Set 'Deny log on as a service' to	Level 1 - Domain	Computer
include 'Guests'	Controller	Configuration\Windows
	Level 1 - Member Server	Settings\Security
		Settings\Local
		Policies/User Rights
		Assignment\Deny log on
Sat 'Dany log on locally' to	Lavel 1 Domain	as a service
include 'Guests'	Controller	Configuration Windows
menude Odests	Level 1 - Member Server	Settings/Security
		Settings/Local
		Policies\User Rights
		Assignment\Denv log on
		locally
Set 'Deny log on through	Level 1 - Domain	Computer
Remote Desktop Services' to	Controller	Configuration\Windows
include 'Guests, Local account'	Level 1 - Member Server	Settings\Security
		Settings\Local
		Policies\User Rights
		Assignment\Deny log on
		through Remote Desktop
Cat 'Enchla commentant and a	Laval 1 Damain	Services
Set Enable computer and user	Level I - Domain	Configuration Windows
delegation'	Level 1 - Member Server	Settings/Security
		Settings\Local
		Policies/User Rights
		Assignment\Enable

		computer and user
		accounts to be trusted
		for delegation
Set 'Force shutdown from a	Level 1 - Domain	Computer
remote system' to	Controller	Configuration Windows
'Administrators'	Level 1 - Member Server	Settings/Security
r tullinguators		Settings/Local
		Policies/User Rights
		Assignment/Force
		shutdown from a remote
		system
Sat 'Concrete security audits' to	Laval 1 Domain	Computer
I OCAL SERVICE	Controller	Configuration Windows
NETWORK SERVICE	Loval 1 Mamban Saman	Softings/Socurity
NET WORK SERVICE	Level 1 - Member Server	Settings/Security
		Policies User Rights
		Assignment\Generate
		security audits
Set Impersonate a client after	Level I - Domain	Computer
authentication' to	Controller	Configuration\Windows
'Administrators, LOCAL	Level 1 - Member Server	Settings\Security
SERVICE, NETWORK		Settings\Local
SERVICE, SERVICE'		Policies\User Rights
		Assignment\Impersonate
		a client after
		authentication
Set 'Increase scheduling	Level 1 - Domain	Computer
priority' to 'Administrators'	Controller	Configuration\Windows
	Level 1 - Member Server	Settings\Security
		Settings\Local
		Policies\User Rights
		Assignment\Increase
		scheduling priority
Set 'Load and unload device	Level 1 - Domain	Computer
drivers' to 'Administrators'	Controller	Configuration\Windows
	Level 1 - Member Server	Settings\Security
		Settings\Local
		Policies\User Rights
		Assignment\Load and
		unload device drivers
Set 'Lock pages in memory' to	Level 1 - Domain	Computer
'No One'	Controller	Configuration\Windows
	Level 1 - Member Server	Settings\Security
		Settings\Local
		Policies\User Rights
		Assignment Lock pages
		in memory
Set 'Manage auditing and	Level 1 - Domain	Computer
security log' to 'Administrators'	Controller	Configuration
	Level 1 - Member Server	Settings\Security

		Settings\Local
		Policies\User Rights
		Assignment\Manage
		auditing and security log
Set 'Modify an object label' to	Level 1 - Domain	Computer
'No One'	Controller	Configuration
	Level 1 - Member Server	Settings\Security
		Settings\Local
		Policies\User Rights
		Assignment/Modify an
		object label
Set 'Modify firmware	Level 1 - Domain	Computer
environment values' to	Controller	Configuration\Windows
'Administrators'	Level 1 - Member Server	Settings\Security
		Settings\Local
		Policies\User Rights
		Assignment
		firmware environment
		values
Set 'Perform volume	Level 1 - Domain	Computer
maintenance tasks' to	Controller	Configuration
'Administrators'	Level 1 - Member Server	Settings\Security
		Settings\Local
		Policies\User Rights
		Assignment\Perform
		volume maintenance
		tasks
Set 'Profile single process' to	Level 1 - Domain	Computer
'Administrators'	Controller	Configuration\Windows
	Level 1 - Member Server	Settings\Security
		Settings\Local
		Policies\User Rights
		Assignment\Profile
		single process
Set 'Profile system performance'	Level 1 - Domain	Computer
to 'Administrators, NT	Controller	Configuration\Windows
SERVICE\WdiServiceHost'	Level 1 - Member Server	Settings\Security
		Settings\Local
		Policies\User Rights
		Assignment\Profile
		system performance
Set 'Replace a process level	Level I - Domain	Computer
token' to 'LOCAL SERVICE,	Controller	Configuration\Windows
NETWORK SERVICE	Level I - Member Server	Settings/Security
		Settings\Local Delicies\Local
		Poincies/User Kignts
		Assignment\Keplace a
Sat Destage Classes 1	Lavel 1. Demok	Computer
directorics' to 'A dministrators'	Level I - Domain	Configuration/Windows
unectories to Administrators	Controller	Configuration windows

	Level 1 - Member Server	Settings\Security
		Settings\Local
		Policies/User Rights
		Assignment\Restore
		files and directories
Set 'Shut down the system' to	Level 1 - Domain	Computer
'Administrators'	Controller	Configuration Windows
	Level 1 - Member Server	Settings/Security
		Settings/Local
		Deligios/User Dights
		Assignment/Shut down
		the system
Set Semanne dinester	Level 1 Demain	Commuter
Set Synchronize difectory	Level 1 - Domain	Computer
service data to No One	Controller	Configuration\Windows
		Settings\Security
		Settings\Local
		Policies\User Rights
		Assignment\Synchronize
		directory service data
	Level 1 - Domain	Computer
Set 'Take ownership of files or	Controller	Configuration\Windows
other objects' to 'Administrators'	Level 1 - Member Server	Settings\Security
		Settings\Local
		Policies\User Rights
		Assignment\Take
		ownership of files or
		other objects
Set 'Accounts: Guest account	Level 1 - Domain	Computer
status' to 'Disabled'	Controller	Configuration\Windows
	Level 1 - Member Server	Settings\Security
		Settings\Local
		Policies
		Options\Accounts:
		Guest account status
Set 'Accounts: Limit local	Level 1 - Domain	HKEY LOCAL MAC
account use of blank passwords	Controller	HINE\System\CurrentC
to console logon only' to	Level 1 - Member Server	ontrolSet/Control/L sa/L i
'Enabled'		mitBlankPasswordUse
Configure 'Accounts: Rename	Level 1 - Domain	Computer
administrator account'	Controller	Configuration Windows
	Level 1 - Member Server	Settings/Security
		Settings/Security
		Dolicies Security
		Options Accounts:
		Denomo administrator
Confirme 14 and the Dames	Lavel 1. Derestr	Computer
Configure Accounts: Kename	Level I - Domain	Computer Configuration Windows
guest account	Controller	Configuration\Windows
	Level I - Member Server	Settings\Security
		Settings\Local

		Policies\Security
		Options Accounts:
		Rename quest account
Sat 'Audit, Shut dawn gustam	Lavel 1 Domein	Auditu
Set Audit. Shut down system	Controllor	Auuit.
immediately if unable to log	Controller	HKEY_LOCAL_MAC
security audits' to 'Disabled'	Level I - Member Server	HINE\System\CurrentC
		ontrolSet\Control\Lsa\cr
		ashonauditfail
		Remediation: Computer
		Configuration\Windows
		Settings\Security
		Settings\Local
		Policies\Security
		Options\Audit: Shut
		down system
		immediately if unable to
		log security audits
Sat 'Davicas: Allowed to format	Level 1 Domain	Andit:
and gigst removable modia' to	Controller	HVEY LOCAL MAC
and eject removable media to		HNE I_LOCAL_MAC
Administrators	Level 1 - Member Server	HINE SORWARE MICROSO
		ft\Windows
		NT\CurrentVersion\Win
		logon\AllocateDASD
		Remediation: Computer
		Configuration Windows
		Sattings/Security
		Settings/Jocal
		Ontional Devices
		Allowed to format and
		Allowed to format and
		eject removable media
Set 'Devices: Prevent users	Level 1 - Domain	Audit:
from installing printer drivers'	Controller	HKEY_LOCAL_MAC
to 'Enabled'	Level 1 - Member Server	HINE\System\CurrentC
		ontrolSet\Control\Print\P
		roviders\LanMan Print
		Services\Servers\AddPri
		nterDrivers
		Remediations Commuter
		Configuration: Computer
		Configuration\windows
		Settings\Security
		Settings\Local
		Policies\Security
		Options\Devices:
		Prevent users from
		installing printer drivers

Set 'Domain controller: Allow server operators to schedule tasks' to 'Disabled'	Level 1 - Domain Controller	Audit: HKEY_LOCAL_MAC HINE\System\CurrentC ontrolSet\Control\Lsa\Su bmitControl Remediation: Computer Configuration\Windows Sattings\Security
		Settings\Local Policies\Security Options\Domain controller: Allow server operators to schedule tasks
Set 'Domain controller: LDAP server signing requirements' to 'Require signing'	Controller	Audit: HKEY_LOCAL_MAC HINE\System\CurrentC ontrolSet\Services\NTD S\Parameters\Idapserveri ntegrity
		Remediation: Computer Configuration/Windows Settings\Security Settings\Local Policies\Security Options\Domain controller: LDAP server signing requirements
Set 'Domain controller: Refuse machine account password changes' to 'Disabled'	Level 1 - Domain Controller	Audit: HKEY_LOCAL_MAC HINE\System\CurrentC ontrolSet\Services\Netlo gon\Parameters\RefuseP asswordChange Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Domain
Set 'Domain member: Digitally	Level 1 - Domain	controller: Refuse machine account password changes Audit:
encrypt or sign secure channel data (always)' to 'Enabled'	Controller Level 1 - Member Server	HKEY_LOCAL_MAC HINE\System\CurrentC ontrolSet\Services\Netlo

		gon\Parameters\requiresi
		gnorseal
		ghorsear
		Pamadiation:
		Computer
		Computer
		Configuration\Windows
		Settings\Security
		Settings\Local
		Policies\Security
		Options\Domain
		member: Digitally
		encrypt or sign secure
		channel data (always)
Set 'Domain member: Digitally	Level 1 - Domain	Audit:
encrypt secure channel data	Controller	HKEY LOCAL MAC
(when possible)' to 'Engbled'	Lovel 1 Member Server	HINE System Current C
(when possible) to Enabled	Level 1 - Member Server	ontrolSot/Services/Notle
		gon/Parameters/sealsecu
		rechannel
		Remediation:
		Computer
		Configuration\Windows
		Settings\Security
		Settings\Local
		Policies\Security
		Options\Domain
		member: Digitally
		encrypt secure channel
		data (when possible)
Set 'Domain member: Disable	Level 1 - Domain	Audit:
machine account password	Controller	HKEY LOCAL MAC
changes' to 'Disabled'	Level 1 - Member Server	HINE\System\CurrentC
changes to Disabled		ontrolSet/Services/Netlo
		gon/Parameters/disablen
		asswordshanga
		asswordenange
		Remediation, Computer
		Canfingentian Windows
		Configuration/windows
		Settings/Security
		Settings\Local
		Policies\Security
		Options\Domain
		member: Disable
		machine account
		password changes
Set 'Domain member:	Level 1 - Domain	Computer
Maximum machine account	Controller	Configuration\Windows
password age' to 60 , but not 0	Level 1 - Member Server	Settings\Security
		Settings\Local
		Policies\Security

		Options Domain	
		mamban Maximum	
		machine account	
		password age	
Set 'Domain member: Require	Level 1 - Domain	Audit:	
strong (Windows 2000 or later)	Controller	HKEY_LOCAL_MAC	
session key' to 'Enabled'	Level 1 - Member Server	HINE\System\CurrentC	
5		ontrolSet\Services\Netlo	
		gon/Parameters/requirest	
		rongkey	
		Toligkey	
		Denne disting Generation	
		Remediation: Computer	
		Configuration\Windows	
		Settings\Security	
		Settings\Local	
		Policies\Security	
		Options\Domain	
		member: Require strong	
		(Windows 2000 or later)	
		session key	
Sat Internative logan: Do not	Lavel 1 Domein	Audit	
Set Interactive logon. Do not	Centuellen	Audit.	
display last user name to	Controller	HKEY_LOCAL_MAC	
'Enabled'	Level I - Member Server	HINE\Software\Microso	
		ft\Windows\CurrentVers	
		ion\Policies\System\Don	
		tDisplayLastUserName	
		Remediation:	
		Computer	
		Configuration Windows	
		Settings/Security	
		Settings/Legal	
		Policies Security	
		Options\Interactive	
		logon: Do not display	
		last user name	
Set 'Interactive logon: Do not	Level 1 - Domain	Audit:	
require CTRL+ALT+DEL' to	Controller	HKEY_LOCAL_MAC	
'Disabled'	Level 1 - Member Server	HINE\Software\Microso	
		ft\Windows\CurrentVers	
		ion/Policies/System/Disa	
		bleCAD	
		Remediation:	
		Computer	
		Computer Configuration Win 1	
		Configuration\windows	
		Settings\Security	
		Settings\Local	
		Policies\Security	
		Options\Interactive	

		logon: Do not require CTRL+ALT+DEL
Set 'Interactive logon: Machine inactivity limit' to 300 second(s), but not 0	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MAC HINE\Software\Microso ft\Windows\CurrentVers ion\Policies\System\Inac tivityTimeoutSecs
		Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Machine inactivity limit
Configure 'Interactive logon: Message text for users attempting to log on'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MAC HINE\Software\Microso ft\Windows\CurrentVers ion\Policies\System\Leg alNoticeText Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Message text for users attempting to log on "This system is owned and operated by GOC. Use is restricted to GOC. Authorised users must comply with the GOC IT Security Policy. Usage is monitored; unauthorized users will
Configure 'Interactive logon: Message title for users attempting to log on'		be prosecuted" Audit: HKEY_LOCAL_MAC HINE\Software\Microso ft\Windows\CurrentVers ion\Policies\System\Leg alNoticeCaption

		Remediation:	
		Computer	
		Configuration Windows	
		Configuration windows	
		Settings\Security	
		Settings\Local	
		Policies	
		Ontions/Interactive	
		Options\interactive	
		logon: Message title for	
		users attempting to log	
		on	
		0.11	
		"Government Online	
		Centre (GOC)"	
Set 'Interactive logon: Number	Level 1 - Domain	Audit:	
Set Interactive logon. Number	Controllor	Audit.	
of previous logons to cache (in	Controller	HKEY_LOCAL_MAC	
case domain controller is not	Level 1 - Member Server	HINE\Software\Microso	
available)' to '3 or fewer		ft\Windows	
logon(s)'		NT\CurrentVersion\Win	
logon(s)			
		logon\cachedlogonscoun	
		t	
		Remediation.	
		Computer	
		Computer	
		Configuration\Windows	
		Settings	
		Settings\Local	
		Policies\Security	
		Options\Interactive	
		logon: Number of	
		previous logons to cache	
		(in case domain	
		(in case domain	
		controller is not	
		available)	
Set 'Interactive logon: Promot		Audit:	
user to change password before		HKEY LOCAL MAC	
user to enange password before			
expiration to between / and 14		HINE\Software\Microso	
days'		ft\Windows	
		NT\CurrentVersion\Win	
		logon\passwordexpirvwa	
		mina	
		Immg	
		Remediation: Computer	
		Configuration\Windows	
		Settings Security	
		Settings\Local	
		Policies	
		<b>Options</b> \Interactive	
		logon: Prompt user to	
		abanga pageward before	
		change password before	
		expiration	

Set 'Microsoft network client:	Level 1 - Domain	Audit:	
Digitally sign communications	Controller	HKEY LOCAL MAC	
(always)' to 'Enabled'	Level 1 - Member Server	HINE\System\CurrentC	
		ontrolSet\Services\Lanm	
		anWorkstation\Paramete	
		rs\RequireSecuritySignat	
		ure	
		Remediation: Computer	
		Configuration\Windows	
		Settings	
		Settings\Local	
		Policies\Security	
		Options\Microsoft	
		network client: Digitally	
		sign communications	
		(always)	
Set 'Microsoft network client:	Level 1 - Domain	Audit:	
Digitally sign communications	Controller	HKEY_LOCAL_MAC	
(if server agrees)' to 'Enabled'	Level 1 - Member Server	HINE\System\CurrentC	
		ontrolSet\Services\Lanm	
		anWorkstation\Paramete	
		rs\EnableSecuritySignat	
		ure	
		Demo listiano Commutan	
		Remediation: Computer	
		Sottings/Socurity	
		Settings\Security	
		Policies Security	
		Options\Microsoft	
		network client: Digitally	
		sign communications (if	
		server agrees)	
Set 'Microsoft network client:	Level 1 - Domain	Audit:	
Send unencrypted password to	Controller	HKEY LOCAL MAC	
third-party SMB servers' to	Level 1 - Member Server	HINE\System\CurrentC	
'Disabled'		ontrolSet\Services\Lanm	
		anWorkstation\Paramete	
		rs\EnablePlainTextPass	
		word	
		Domodiation Comments	
		Configuration: Computer	
		Sottings Socurity	
		Settings Security	
		Policies/Security	
		Options\Microsoft	
		network client: Send	
		unencrypted password to	
		third-party SMB servers	

Set 'Microsoft network server:	Level 1 - Domain	Audit:	
Amount of idle time required	Controller	HKEY_LOCAL_MAC	
before suspending session' to '5	Level 1 - Member Server	HINE\System\CurrentC	
minute(s)'		ontrolSet\Services\LanM	
		anServer\Parameters\aut	
		odisconnect	
		Remediation: Computer	
		Configuration\Windows	
		Settings\Security	
		Settings\Local	
		Policies\Security	
		Options\Microsoft	
		network server: Amount	
		of idle time required	
		before suspending	
		session	
Set 'Microsoft network server:	Level 1 - Domain	Audit:	
Digitally sign communications	Controller	HKEY_LOCAL_MAC	
(always) to Enabled	Level 1 - Member Server	HINE\System\CurrentC	
		ontrolSet\Services\LanM	
		anServer\Parameters\req	
		uiresecuritysignature	
		Remediation:	
		Computer	
		Configuration Windows	
		Settings/Security	
		Settings/Local	
		Policies	
		Options\Microsoft	
		network server: Digitally	
		sign communications	
		(always)	
Set 'Microsoft network server:	Level 1 - Domain	Audit:	
Digitally sign communications	Controller	HKEY_LOCAL_MAC	
(if client agrees)' to 'Enabled'	Level 1 - Member Server	HINE\System\CurrentC	
		ontrolSet\Services\LanM	
		anServer\Parameters\ena	
		blesecuritysignature	
		Remediation: Computer	
		Configuration/Windows	
		Settings\Security	
		Settings\Local	
		Policies Security	
		network server: Digitally	
		sign communications (if	
		client agrees)	

Set 'Microsoft network server:	Level 1 - Domain	Audit:	
Disconnect clients when logon	Controller	HKEY LOCAL MAC	
hours expire' to 'Enabled'	Level 1 - Member Server	HINE\System\CurrentC	
1		ontrolSet\Services\LanM	
		anServer\Parameters\ena	
		bleforcedlogoff	
		onereneedingen	
		Remediation:	
		Computer	
		Configuration\Windows	
		Settings/Security	
		Settings\Local	
		Policies	
		Options\Microsoft	
		network server	
		Disconnect clients when	
		logon hours expire	
Set 'Microsoft network server'	Level 1 - Domain	Audit:	
Server SPN target name	Controller	HKEY LOCAL MAC	
validation level' to 'Accept if	Level 1 - Member Server	HINE\System\CurrentC	
provided by client'		ontrolSet\Services\LanM	
provided by cheft		anServer\Parameters\SM	
		RServerNameHardening	
		I evel	
		Lever	
		Remediation:	
		Computer	
		Configuration Windows	
		Settings\Security	
		Settings\Local	
		Policies	
		Options\Microsoft	
		network server: Server	
		SPN target name	
		validation level	
Set 'MSS: (AutoAdminLogon)	Level 1 - Domain	Audit:	
Enable Automatic Logon (not	Controller	HKEY LOCAL MAC	
recommended)' to 'Disabled'	Level 1 - Member Server	HINE\Software\Microso	
recommended) to Disabled		ft/Windows	
		NT\CurrentVersion\Win	
		logon\AutoAdminLogon	
		logon (r tator taninin20gon	
		Remediation:	
		Computer	
		Configuration\Windows	
		Settings\Security	
		Settings\Local	
		Policies	
		Options\MSS:	
		(AutoAdminLogon)	
		Enable Automatic	

		Logon (not
		recommended)
Set 'MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)' to 'Highest protection, source routing is completely disabled'	Level 1 - Domain Controller Level 1 - Member Server	recommended)         Audit:         HKEY_LOCAL_MAC         HINE\System\CurrentC         ontrolSet\Services\Tcpip         6\Parameters\DisableIPS         ourceRouting         Remediation: Computer         Configuration\Windows         Settings\Security         Settings\Local         Policies\Security         Options\MSS:
		(DisableIPSourceRoutin g IPv6) IP source routing protection level (protects against packet spoofing)
Set 'MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)' to 'Highest protection, source routing is completely disabled'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MAC HINE\System\CurrentC ontrolSet\Services\Tcpip \Parameters\DisableIPSo urceRouting
		Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\MSS: (DisableIPSourceRoutin g) IP source routing protection level (protects against packet spoofing)
Set MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)' to 'Enabled'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MAC HINE\SYSTEM\Current ControlSet\Control\Sessi on Manager\SafeDllSearch Mode Remediation:
		Computer Configuration\Windows Settings\Security Settings\Local Policies\Security

		Options\MSS:	
		(SafeDllSearchMode)	
		Enable Safe DLL search	
C-4 DACC	Land 1. Damain	mode (recommended)	
(ScreenSaverGracePeriod) The time in seconds before the screen saver grace period	Controller Level 1 - Member Server	HKEY_LOCAL_MAC HINE\Software\Microso ft\Windows	
expires to 300 seconds		NI\CurrentVersion\Win logon\ScreenSaverGrace Period	
		Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\MSS:	
		(ScreenSaverGracePerio d) The time in seconds before the screen saver grace period expires	
Set 'MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning' to '90% or less'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MAC HINE\SYSTEM\Current ControlSet\Services\Eve ntlog\Security\WarningL evel	
		Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning	
Set 'Network access: Allow anonymous SID/Name translation' to 'Disabled'	Level 1 - Domain Controller Level 1 - Member Server	Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Allow anonymous SID/Name translation	

Set 'Network access: Do not	Level 1 - Domain	Audit:	
allow anonymous enumeration	Controller	HKEY_LOCAL_MAC	
of SAM accounts' to 'Enabled'	Level 1 - Member Server	HINE\System\CurrentC	
		ontrolSet\Control\Lsa\R	
		estrictAnonymousSAM	
		Remediation:	
		Computer	
		Configuration\Windows	
		Settings\Security	
		Options/Network access:	
		Do not allow	
		anonymous enumeration	
		of SAM accounts	
Set 'Network access: Do not	Level 1 - Domain	Audit:	
allow anonymous enumeration	Controller	HKEY LOCAL MAC	
of SAM accounts and shares' to	Level 1 - Member Server	HINE\System\CurrentC	
'Enabled'		ontrolSet\Control\Lsa\R	
		estrictAnonymous	
		Remediation:	
		Computer	
		Configuration\Windows	
		Settings\Security	
		Settings\Local	
		Policies\Security	
		Do not allow	
		anonymous enumeration	
		of SAM accounts and	
		shares	
Set 'Network access: Let	Level 1 - Domain	Audit:	
Everyone permissions apply to	Controller	HKEY_LOCAL_MAC	
anonymous users' to 'Disabled'	Level 1 - Member Server	HINE\System\CurrentC	
		ontrolSet\Control\Lsa\E	
		veryoneIncludesAnony	
		mous	
		Configuration: Computer	
		Settings Security	
		Settings/Local	
		Policies\Security	
		Options\Network access	
		Let Evervone	
		permissions apply to	
		anonymous users	

Configure 'Network Access:	Level 1 - Domain	Audit:	
Named Pipes that can be	Controller	HKEY LOCAL MAC	
accessed anonymously'	Level 1 - Member Server	HINE\SYSTEM\Current	
		ControlSet\Services\Lan	
		ManServer\Parameters\	
		NullSessionPipes	
		r tulibebbiolit ipeb	
		Remediation: Computer	
		Configuration Windows	
		Settings\Security	
		Settings/Decalty	
		Policies	
		Options	
Set 'Network access: Remotely	Level 1 Domain	The recommended state	
accessible registry paths'	Controller	for this setting is:	
accessible registry paths	Level 1 - Member Server	System/CurrentControlS	
		et/Control/ProductOntio	
		IIS System\CurrentControlS	
		at/Control/Server	
		Applications	
		Software\Microsoft\Win	
		dows	
		NT\CurrentVersion	
		Audit	
		HKEV LOCAL MAC	
		HINE\System\CurrentC	
		ontrolSet\Control\Secure	
		PipeServers/Winreg/All	
		owedEvactPaths\Machin	
		C	
		Remediation: Computer	
		Configuration Windows	
		Settings\Security	
		Settings/Local	
		Policies/Security	
		Options/Network access:	
		Remotely accessible	
		registry paths	
Set 'Network access: Remotely	Level 1 - Domain	The recommended state	
accessible registry paths and	Controller	for this setting is:	
sub-paths'	Level 1 - Member Server	System\CurrentControlS	
Paulo		et\Control\Print\Printers	
		System\CurrentControlS	
		et\Services\Eventlog	
		Software\Microsoft\OL	
		AP Server	
		Software\Microsoft\Win	
		dows	

		NT\CurrentVersion\Print	
		Software\Microsoft\Win	
		dows	
		NT\CurrentVersion\Win	
		dows	
		System\CurrentControlS	
		et/Control/ContentIndex	
		System/CurrentControlS	
		et/Control/Terminal	
		Server	
		System\CurrentControlS	
		at/Control/Torminal	
		Somer/HearConfig	
		Server\UserComing	
		system/CurrentControls	
		et/Control/Terminal	
		Server\DefaultUserConfi	
		guration	
		Software\Microsoft\Win	
		aows	
		N I \Current Version\Perfl	
		1b	
		System\CurrentControlS	
		et\Services\SysmonLog	
		Audit:	
		HKEY LOCAL MAC	
		HINE\Svstem\CurrentC	
		ontrolSet\Control\Secure	
		PipeServers\Winreg\All	
		owedPaths\Machine	
		Remediation:	
		Computer	
		Configuration\Windows	
		Settings\Security	
		Settings\Local	
		Policies	
		Options\Network access:	
		Remotely accessible	
		registry paths and sub-	
		paths	
Set 'Network access: Restrict	Level 1 - Domain	Audit:	
anonymous access to Named	Controller	HKEY LOCAL MAC	
Pipes and Shares' to 'Enabled'	Level 1 - Member Server	HINE\System\CurrentC	
r Z to Z		ontrolSet\Services\LanM	
		anServer\Parameters\rest	
		rictnullsessaccess	
		Remediation: Computer	
		Configuration\Windows	
		Settings\Security	

		Settings\Local Policies\Security Options\Network access: Restrict anonymous
		access to Named Pipes and Shares
Set 'Network access: Shares that can be accessed anonymously' to 'None'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MAC HINE\System\CurrentC ontrolSet\Services\LanM anServer\Parameters\Nul lSessionShares
		Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Shares that can be accessed anonymously
Set 'Network access: Sharing and security model for local accounts' to 'Classic - local users authenticate as themselves'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MAC HINE\System\CurrentC ontrolSet\Control\Lsa\Fo rceGuest
		Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Sharing and security model for local accounts
Set 'Network security: Allow Local System to use computer identity for NTLM' to 'Enabled'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MAC HINE\System\CurrentC ontrolSet\Control\Lsa\U seMachineId
		Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Allow Local System to use computer identity for NTLM

Set 'Network security: Allow	Level 1 - Domain	Audit:	
LocalSystem NULL session	Controller	HKEY_LOCAL_MAC	
Tanback to Disabled	Level I - Mellider Server	ontrolSet\Control\Lsa\M	
		SV1_0\allownullsessionf	
		allback	
		Remediation: Computer	
		Configuration\Windows	
		Settings\Security	
		Settings\Local	
		Policies\Security	
		security: Allow	
		LocalSystem NULL	
		session fallback	
Set 'Network Security: Allow	Level 1 - Domain	Audit:	
PKU2U authentication requests	Controller	HKEY_LOCAL_MAC	
to this computer to use online	Level I - Member Server	HINE\System\CurrentC	
identifies to Disabled		u2u\AllowOnlineID	
		Remediation: Computer	
		Configuration\Windows	
		Settings\Security	
		Policies\Security	
		<b>Options</b> \Network	
		Security: Allow PKU2U	
		authentication requests	
		to this computer to use	
Set 'Network Security:	Level 1 - Domain	Audit:	
Configure encryption types	Controller	HKEY_LOCAL_MAC	
allowed for Kerberos' to	Level 1 - Member Server	HINE\Software\Microso	
'RC4\AES128\AES256\Future		ft\Windows\CurrentVers	
types		10n\Policies\System\Ker beros\Parameters\Suppor	
		tedEncryptionTypes	
		to a line i priori i pros	
		Remediation: Computer	
		Configuration\Windows	
		Settings\Security	
		Policies/Security	
		Options\Network	
		Security: Configure	
		encryption types allowed	
Set 'Network security: Do not	Level 1 - Domain	10r Kerberos	
store LAN Manager hash value	Controller	HKEY_LOCAL_MAC	

on next password change' to 'Enabled'	Level 1 - Member Server	HINE\System\CurrentC ontrolSet\Control\Lsa\N oLMHash Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Do not store LAN Manager hash value on next password change
Set 'Network security: Force logoff when logon hours expire' to 'Enabled'	Level 1 - Domain Controller Level 1 - Member Server	Remediation:ComputerConfiguration\Windows Settings\SecuritySettings\LocalPolicies\SecurityOptions\Networksecurity: Force logoffwhen logon hoursexpire
Set 'Network security: LAN Manager authentication level' to 'Send NTLMv2 response only. Refuse LM & NTLM'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MAC HINE\System\CurrentC ontrolSet\Control\Lsa\L mCompatibilityLevel Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Network security: LAN Manager authentication level
Set 'Network security: LDAP client signing requirements' to 'Negotiate signing' or higher	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MAC HINE\System\CurrentC ontrolSet\Services\LDA P\LDAPClientIntegrity Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Network

		security: LDAP client signing requirements
Set 'Network security:	Level 1 - Domain	Audit
Minimum session security for NTLM SSP based (including secure RPC) clients' to 'Require NTLMv2 session security,Require 128-bit encryption'	Controller Level 1 - Member Server	HKEY_LOCAL_MAC HINE\System\CurrentC ontrolSet\Control\Lsa\M SV1_0\NTLMMinClient Sec
		Remediation: Computer Configuration\Windows Settings\Security
		Policies\Security Options\Network
		session security for NTLM SSP based (including secure RPC)
Set 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' to 'Require NTLMv2 session security,Require 128-bit	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MAC HINE\System\CurrentC ontrolSet\Control\Lsa\M SV1_0\NTLMMinServe rSec
encryption		Remediation: Computer Configuration\Windows Settings\Security
		Policies\Security Options\Network security: Minimum session security for NTLM SSP based
		(including secure RPC) servers
Set 'Recovery console: Allow automatic administrative logon' to 'Disabled'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MAC HINE\Software\Microso ft\Windows NT\CurrentVersion\Setu p\RecoveryConsole\secu ritylevel
		Remediation: Computer Configuration\Windows Settings\Security

		Settings\Local Policies\Security Options\Recovery console: Allow
		automatic administrative
Set 'Recovery console: Allow floppy copy and access to all drives and all folders' to 'Disabled'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MAC HINE\Software\Microso ft\Windows NT\CurrentVersion\Setu p\RecoveryConsole\setc ommand
		Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Recovery console: Allow floppy copy and access to all drives and all folders
Set 'Shutdown: Allow system to be shut down without having to log on' to 'Disabled'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MAC HINE\Software\Microso ft\Windows\CurrentVers ion\Policies\System\Shut downWithoutLogon Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Shutdown: Allow system to be shut down without having to log on
Set 'System objects: Require case insensitivity for non- Windows subsystems' to 'Enabled'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MAC HINE\System\CurrentC ontrolSet\Control\Sessio n Manager\Kernel\ObCase Insensitive Remediation: Computer Configuration\Windows Settings\Security Settings\Local

		Policies\Security
		Options\System objects:
		Require case
		insensitivity for non-
		Windows subsystems
Set 'System objects: Strengthen	Level 1 - Domain	Audit:
default permissions of internal	Controller	HKEY LOCAL MAC
system objects (e.g. Symbolic	Level 1 - Member Server	HINE\System\CurrentC
Links)' to 'Enabled'		ontrolSet/Control/Sessio
Links) to Lindoled		n n
		II Managar/DrotactionMod
		Wanager \F TotectionWood
		e
		Remediation: Computer
		Configuration\Windows
		Settings\Security
		Settings\Local
		Policies\Security
		Options\System objects:
		Strengthen default
		permissions of internal
		system objects (e.g.
		Symbolic Links)
Set 'User Account Control:	Level 1 - Domain	Audit:
Admin Approval Mode for the	Controller	HKEY LOCAL MAC
Built-in Administrator account'	Level 1 - Member Server	HINE\Software\Microso
to 'Enabled'		ft\Windows\CurrentVers
		ion/Policies/System/Filte
		rAdministratorToken
		Remediation: Computer
		Configuration/Windows
		Settings/Security
		Settings/Local
		Policies/Security
		Options/User Account
		Control: Admin
		Control: Admin
		Approval Mode for the
		Built-in Administrator
Set User Account Control:	Level I - Domain	Audit:
Allow UIAccess applications to	Controller	HKEY_LOCAL_MAC
prompt for elevation without	Level 1 - Member Server	HINE\SOFTWARE\Mic
using the secure desktop' to		rosoft\Windows\Current
'Disabled'		Version\Policies\System
		\EnableUIADesktopTog
		gle
		Remediation: Computer
		Configuration\Windows
		Settings\Security

		Settings\Local Policies\Security Options\User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop	
Set 'User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode' to 'Prompt for consent on the secure desktop'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MAC HINE\Software\Microso ft\Windows\CurrentVers ion\Policies\System\Con sentPromptBehaviorAd min Remediation: Computer	
		Configuration\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode	
Set 'User Account Control: Behavior of the elevation prompt for standard users' to 'Automatically deny elevation requests'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MAC HINE\Software\Microso ft\Windows\CurrentVers ion\Policies\System\Con sentPromptBehaviorUse r	
		Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Behavior of the elevation prompt for standard users	
Set 'User Account Control: Detect application installations and prompt for elevation' to 'Enabled'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MAC HINE\Software\Microso ft\Windows\CurrentVers ion\Policies\System\Ena bleInstallerDetection	

Set 'User Account Control: Only elevate UIAccess	Level 1 - Domain Controller	Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Detect 
applications that are installed in secure locations' to 'Enabled'	Level 1 - Member Server	HINE\Software\Microso ft\Windows\CurrentVers ion\Policies\System\Ena bleSecureUIAPaths Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Only elevate UIAccess applications that are installed in secure locations
Set 'User Account Control: Run all administrators in Admin Approval Mode' to 'Enabled'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MAC HINE\Software\Microso ft\Windows\CurrentVers ion\Policies\System\Ena bleLUA Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Run all administrators in Admin Approval Mode
Set 'User Account Control: Switch to the secure desktop when prompting for elevation' to 'Enabled'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MAC HINE\Software\Microso ft\Windows\CurrentVers ion\Policies\System\Pro mptOnSecureDesktop Remediation: Computer Configuration\Windows

		Settings\Security Settings\Local Policies\Security Options\User Account Control: Switch to the secure desktop when	
Set 'User Account Control: Virtualize file and registry write failures to per-user locations' to 'Enabled'	Level 1 - Domain Controller Level 1 - Member Server	prompting for elevation         Audit:         HKEY_LOCAL_MAC         HINE\Software\Microso         ft\Windows\CurrentVers         ion\Policies\System\Ena         bleVirtualization         Remediation: Computer	
		Configuration/Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Virtualize file and registry write failures to per-user locations	
Set 'Windows Firewall: Domain: Firewall state' to 'On (recommended)'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MAC HINE\Software\Policies\ Microsoft\WindowsFire wall\DomainProfile\Ena bleFirewall Remediation: Computer	
		Configuration/Windows Settings/Security Settings/Windows Firewall with Advanced Security/Windows Firewall with Advanced Security/Windows Firewall Properties/Domain Profile/Windows Firewall: Domain: Firewall state	
Set 'Windows Firewall: Domain: Inbound connections' to 'Block (default)'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MAC HINE\Software\Policies\ Microsoft\WindowsFire wall\DomainProfile\Def aultInboundAction	

		Remediation: Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Windows Firewall: Domain;	
		Inbound connections	
Set 'Windows Firewall: Domain: Outbound connections' to 'Allow (default)'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MAC HINE\Software\Policies\ Microsoft\WindowsFire wall\DomainProfile\Def aultOutboundAction	
		Remediation: Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Windows Firewall: Domain: Outbound connections	
Set 'Windows Firewall: Domain: Display a notification' to 'Yes (default)'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MAC HINE\Software\Policies\ Microsoft\WindowsFire wall\DomainProfile\Disa bleNotifications	
		Remediation: Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Windows	

		Firewall: Domain:
		Display a notification
Set 'Windows Firewall: Domain: Allow unicast response' to 'No'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MAC HINE\Software\Policies\ Microsoft\WindowsFire wall\DomainProfile\Disa bleUnicastResponsesTo MulticastBroadcast
		Remediation: Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Windows Firewall: Domain: Allow unicast response
Set 'Windows Firewall: Domain: Apply local firewall rules' to 'Yes (default)'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MAC HINE\Software\Policies\ Microsoft\WindowsFire wall\DomainProfile\Allo wLocalPolicyMerge Remediation: Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Windows Firewall: Domain: Apply local firewall rules
Set 'Windows Firewall: Domain: Apply local connection security rules' to 'Yes (default)'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MAC HINE\Software\Policies\ Microsoft\WindowsFire wall\DomainProfile\Allo wLocalIPsecPolicyMerg e

Set 'Windows Firewall: Domain: Logging: Name' to '%SYSTEMROOT%\System32 \logfiles\firewall\domainfw.log'	Level 1 - Domain Controller Level 1 - Member Server	Remediation: Computer Configuration/Windows Settings/Security Settings/Windows Firewall with Advanced Security/Windows Firewall with Advanced Security/Windows Firewall Properties/Domain Profile/Windows Firewall: Domain: Apply local connection security rules Audit: HKEY_LOCAL_MAC HINE/Software\Policies/ Microsoft/WindowsFire wall/DomainProfile/Log ging/LogFilePath Remediation: To establish the recommended configuration via GP, set the following UI path to %SYSTEMROOT%/Sys tem32\logfiles\firewall\d omainfw.log Computer Configuration/Windows Settings/Security Settings/Windows Firewall with Advanced Security/Windows Firewall with Advanced Security/Windows Firewall with Advanced Security/Windows Firewall with Advanced Security/Windows Firewall with Advanced Security/Windows Firewall Nomain Profile/Logging/Windo ws Firewall: Domain: Logging: Name	
Set 'Windows Firewall: Domain: Logging: Size limit (KB)' to '16,384 KB or greater '	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MAC HINE\Software\Policies\ Microsoft\WindowsFire	

		wall\DomainProfile\Log	
		ging/LogEiloSizo	
		ging\Logimesize	
		To set all the large	
		To establish the	
		recommended	
		configuration via GP, set	
		the following UI path to	
		16,384 KB or greater.	
		Computer	
		Configuration\Windows	
		Settings\Security	
		Settings\Windows	
		Firewall with Advanced	
		Security\Windows	
		Firewall with Advanced	
		Security\Windows	
		Firewall	
		Properties\Domain	
		Profile\Logging\Windo	
		ws Firewall: Domain:	
		Logging: Size limit	
		(KB)	
Set 'Windows Firewall:	Level 1 - Domain	Audit:	
Domain: Logging: Log dropped	Controller	HKEY LOCAL MAC	
nackets' to 'Yes'	Level 1 - Member Server	HINE\Software\Policies\	
		Microsoft\WindowsFire	
		wall\DomainProfile\Log	
		ging I og Dropped Packet	
		s	
		5	
		Remediation: Computer	
		Configuration Windows	
		Sottings Socurity	
		Settings\Windows	
		Eirowell with Advanced	
		Security Windows	
		Eirowell with Advenced	
		Security Windows	
		Security/windows	
		Properties Domain	
		Profile/Logging/Winds	
		ws Firewall: Domain:	
		Logging: Log aropped	
		packets	
Set Windows Firewall:	Level I - Domain	Audit:	
Domain: Logging: Log	Controller	HKEY_LOCAL_MAC	
successful connections' to 'Yes'	Level I - Member Server	HINE\Software\Policies\	
		Microsoft\WindowsFire	
		wall\DomainProfile\Log	

-		
	ging\LogSuccessfulCon nections	
	Remediation: Computer Configuration/Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Logging\Windo	
	ws Firewall: Domain: Logging: Log successful	
	connections	
Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MAC HINE\Software\Policies\ Microsoft\WindowsFire wall\PrivateProfile\Enab leFirewall	
Level 1 Domein	Remediation: Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Windows Firewall: Private: Firewall state	
Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MAC HINE\Software\Policies\ Microsoft\WindowsFire wall\PrivateProfile\Defa ultInboundAction Remediation: To establish the recommended configuration via GP, set the following LI path to	
	Level 1 - Domain Controller Level 1 - Member Server	ging\LogSuccessfulCon nectionsRemediation: Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows FirewallLevel 1 - Domain ControllerLevel 1 - Member ServerLevel 1 - Member ServerMicrosoft\Windows FirewallRemediation: Configuration\Windows FirewallLevel 1 - Member ServerLevel 1 - Member ServerMicrosoft\Windows FirewallRemediation: Configuration\Windows FirewallRemediation: Configuration\Windows FirewallRemediation: Configuration\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\W

		Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Windows Firewall: Private: Inbound connections	
Set 'Windows Firewall: Private:	Level 1 - Domain	Audit:	
Outbound connections' to 'Allow (default)'	Controller Level 1 - Member Server	HKEY_LOCAL_MAC HINE\Software\Policies\ Microsoft\WindowsFire wall\PrivateProfile\Defa ultOutboundAction	
		Remediation: To establish the recommended configuration via GP, set the following UI path to Allow (default).	
		Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Windows Firewall: Private:	
Set 'Windows Firewall: Private: Display a notification' to 'Yes (default)'	Level 1 - Domain Controller Level 1 - Member Server	Outbound connections         Audit:         HKEY_LOCAL_MAC         HINE\Software\Policies\         Microsoft\WindowsFire         wall\PrivateProfile\Disa         bleNotifications         Remediation:         To establish the	

		configuration via GP, set the following UI path to Yes (default).	
		Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Windows Firewall: Private: Display a notification	
Set 'Windows Firewall: Private:	Level 1 - Domain	Audit:	
Allow unicast response' to 'No'	Controller Level 1 - Member Server	HKEY_LOCAL_MAC HINE\Software\Policies\ Microsoft\WindowsFire wall\PrivateProfile\Disa bleUnicastResponsesTo MulticastBroadcast	
		Remediation: Computer Configuration\Windows Settings\Security	
		Settings\Windows Firewall with Advanced	
		Security\Windows Firewall with Advanced	
		Security\Windows	
		Properties\Private Profile\Windows Firewall: Private: Allow	
Set 'Windows Firewall: Private: Apply local firewall rules' to 'Yes (default)'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MAC HINE\Software\Policies\ Microsoft\WindowsFire wall\PrivateProfile\Allo wLocalPolicyMerge	
		Remediation: Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows	

		Firewall with Advanced	
		Security\Windows	
		Firewall	
		Properties\Private	
		Profile\Windows	
		Firewall: Private: Apply	
		local firewall rules	
Set 'Windows Firewall: Private:	Level 1 - Domain	Audit:	
Apply local connection security	Controller	HKEY_LOCAL_MAC	
rules' to 'Yes (default)'	Level 1 - Member Server	HINE\Software\Policies\	
		Microsoft\WindowsFire	
		wall\PrivateProfile\Allo	
		wLocalIPsecPolicyMerg	
		e	
		Remediation: Computer	
		Configuration\Windows	
		Settings\Security	
		Settings\Windows	
		Firewall with Advanced	
		Security\Windows	
		Firewall with Advanced	
		Security\Windows	
		Firewall	
		Properties\Private	
		Profile\Windows	
		Firewall: Private: Apply	
		local connection security	
		rules	
Set 'Windows Firewall: Private:	Level 1 - Domain	Audit:	
Logging: Name' to	Controller	HKEY_LOCAL_MAC	
'%SYSTEMROOT%\System32	Level 1 - Member Server	HINE\Software\Policies\	
\logfiles\firewall\privatefw.log'		Microsoft\WindowsFire	
		wall\PrivateProfile\Logg	
		ing\LogFilePath	
		Remediation:	
		To establish the	
		recommended	
		configuration via GP, set	
		the following UI path to	
		%SYSTEMROOT%\Sys	
		tem32\logfiles\firewall\p	
		rivatefw.log.	
		Computer	
		Configuration\Windows	
		Settings	
		Settings\Windows	
		Firewall with Advanced	

		Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private	
		Profile\Logging\Windo ws Firewall: Private:	
Set 'Windows Firewall: Private: Logging: Size limit (KB)' to '16,384 KB or greater'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MAC HINE\Software\Policies\ Microsoft\WindowsFire wall\PrivateProfile\Logg ing\LogFileSize	
		Remediation: Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Logging\Windo ws Firewall: Private: Logging: Size limit	
		(KB)	
Set 'Windows Firewall: Private: Logging: Log dropped packets' to 'Yes'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MAC HINE\Software\Policies\ Microsoft\WindowsFire wall\PrivateProfile\Logg ing\LogDroppedPackets	
		Remediation: Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Logging\Windo ws Firewall: Private:	
		packets	

Set 'Windows Firewall: Private:	Level 1 - Domain	Audit:	
Logging: Log successful	Controller	HKEY_LOCAL MAC	
connections' to 'Yes'	Level 1 - Member Server	HINE\Software\Policies\	
		Microsoft\WindowsFire	
		wall\PrivateProfile\Logg	
		ing\LogSuccessfulConne	
		ctions	
		ctions	
		Remediation:	
		Computer	
		Configuration	
		Settings\Security	
		Settings\Windows	
		Firewall with Advanced	
		Security Windows	
		Firewall with Advanced	
		Security Windows	
		Firewall	
		Properties Private	
		Profile/Logging/Windo	
		ws Firewall: Private:	
		Logging: Log successful	
		connections	
Set 'Windows Firewall: Public:	Level 1 - Domain	Audit:	
Firewall state' to 'On	Controller	HKEY LOCAL MAC	
(recommended)'	Level 1 - Member Server	HINE Software Policies	
(recommended)	Lever 1 - Member Server	Microsoft/WindowsFire	
		wall\PublicProfile\Enabl	
		eFirewall	
		ernewan	
		Remediation: Computer	
		Configuration Windows	
		Settings\Security	
		Settings\Windows	
		Firewall with Advanced	
		Security/Windows	
		Firewall with Advanced	
		Security/Windows	
		Firewall	
		Properties Public	
		Profile/Windows	
		Firewall: Public:	
		Firewall state	
Set 'Windows Firewall' Public'	Level 1 - Domain	Andit	
Inbound connections' to 'Block	Controller	HKEY LOCAL MAC	
(default)'	Level 1 - Member Server	HINE\Software\Policies	
		Microsoft/WindowsFire	
		wall/PublicProtile/Detail	
		wall\PublicProfile\Defau	

		Remediation: Computer	
		Configuration	
		Configuration windows	
		Settings\Security	
		Settings\Windows	
		Firewall with Advanced	
		Compiled Win dome	
		Security\windows	
		Firewall with Advanced	
		Security\Windows	
		Firewall	
		Properties\Public	
		Profile\Windows	
		Firewall: Public:	
		Inbound connections	
	L LL D '		
Set Windows Firewall: Public:	Level I - Domain	Audit:	
Outbound connections' to	Controller	HKEY_LOCAL_MAC	
'Allow (default)'	Level 1 - Member Server	HINE\Software\Policies\	
		Microsoft/WindowsFire	
		wall\PublicProfile\Defau	
		ltOutboundAction	
		Remediation: Computer	
		C C VV 1	
		Configuration windows	
		Settings	
		Settings\Windows	
		Firewall with Advanced	
		Security\Windows	
		Firewall with Advanced	
		Security\Windows	
		Firewall	
		Properties\Public	
		Profile\Windows	
		Firewall: Public:	
		Outhound connections	
	L 11 D :		
Set Windows Firewall: Public:	Level I - Domain	Audit:	
Display a notification' to 'Yes'	Controller	HKEY_LOCAL_MAC	
	Level 1 - Member Server	HINE\Software\Policies\	
		Microsoft Windows Fire	
		wall\PublicProfile\Disab	
		leNotifications	
		Remediation: Computer	
		Configuration. Computer	
		Configuration\Windows	
		Settings\Security	
		Settings\Windows	
		Firewall with Advanced	
		Constant With Auvanceu	
		Security\windows	
		Firewall with Advanced	
		Security\Windows	
		Firewall	
		Duonoutice Desk12	
		Properties\Public	
		Profile\Windows	

		Firewall: Public: Display
		a notification
Set 'Windows Firewall: Public:	Level 1 - Domain	Audit:
Allow unicast response' to 'No'	Controller	HKEY_LOCAL_MAC
	Level 1 - Member Server	HINE\Software\Policies\
		Microsoft\WindowsFire
		wall\PublicProfile\Disab
		leUnicastResponsesToM
		ulticastBroadcast
		Remediation: Computer
		Configuration
		Settings\Security
		Settings\Windows
		Firewall with Advanced
		Security/Windows
		Firewall with Advanced
		Security\Windows
		Firewall
		Properties\Public
		Profile\Windows
		Firewall: Public: Allow
		unicast response
Set 'Windows Firewall: Public:	Level 1 - Domain	Audit:
Apply local firewall rules' to	Controller	HKEY_LOCAL_MAC
'Yes (default)'	Level 1 - Member Server	HINE\Software\Policies\
		Microsoft\WindowsFire
		wall\PublicProfile\Allow
		LocalPolicyMerge
		Remediation: Computer
		Configuration\Windows
		Settings\Security
		Settings\Windows
		Firewall with Advanced
		Security\Windows
		Firewall with Advanced
		Security\Windows
		Firewall
		Properties\Public
		Profile/Windows
		Firewall: Public: Apply
Cod WV's doesn't F' 11 D 11'	Land 1 Day	local firewall rules
Set Windows Firewall: Public:	Level I - Domain	Audit:
Apply local connection security	Lough 1 Momber Server	INE I_LUCAL_WAU
	Level 1 - Member Server	Microsoft/WindowsEiro
		well\DublicDrefile\Allow
		wan\rubicrioine\Anow
		Locan see oneyweige
1	1	

		Pamadiation: Computer	
		C C VV	
		Configuration\Windows	
		Settings	
		Settings\Windows	
		Firewall with Advanced	
		Security\Windows	
		Firewall with Advanced	
		Constitution Advanced	
		Security\windows	
		Firewall	
		Properties\Public	
		Profile\Windows	
		Firewall: Public: Apply	
		local connection security	
		rulos	
		Tules	
Set 'Windows Firewall: Public:	Level I - Domain	Audit:	
Logging: Name' to	Controller	HKEY_LOCAL_MAC	
'%SYSTEMROOT%\System32	Level 1 - Member Server	HINE\Software\Policies\	
\logfiles\firewall\publicfw.log'		Microsoft\WindowsFire	
hogenes (men mill some miss		wall\PublicProfile\Loggi	
		wan't uoner forne (Loggi	
		ng\Logrneraui	
		Remediation: Computer	
		Configuration\Windows	
		Settings	
		Settings\Windows	
		Firewall with Advanced	
		Constitution Advanced	
		Security\windows	
		Firewall with Advanced	
		Security\Windows	
		Firewall	
		Properties\Public	
		Profile I ogging Windo	
		we Eirowell: Dublic:	
		ws Filewall: Public:	
		Logging: Name	
Set 'Windows Firewall: Public:	Level 1 - Domain	Audit:	
Logging: Size limit (KB)' to	Controller	HKEY_LOCAL_MAC	
'16.384 KB or greater'	Level 1 - Member Server	HINE\Software\Policies\	
		Microsoft\WindowsFire	
		well\DublicDrofile\Loggi	
		ng\LogFileSize	
		Remediation: Computer	
		Configuration\Windows	
		Settings	
		Settings\Windows	
		Firowall with Advanced	
		Constant with Advanced	
		Security\windows	
		Firewall with Advanced	
		Security\Windows	
		Firewall	
		Properties\Public	
		Properties	

		Profile Logging Windo
		ws Firewall: Public:
		Logging: Size limit
		(VD)
Set Windows Firewall: Public:	Level I - Domain	Audit:
Logging: Log dropped packets'	Controller	HKEY_LOCAL_MAC
to 'Yes'	Level 1 - Member Server	HINE\Software\Policies\
		Microsoft\WindowsFire
		wall\PublicProfile\Loggi
		ng\LogDroppedPackets
		Remediation: Computer
		Configuration Windows
		Sottings/Socurity
		Settings/Windows
		Einenen II erith Advenue d
		Firewall with Advanced
		Security\Windows
		Firewall with Advanced
		Security\Windows
		Firewall
		Properties\Public
		Profile\Logging\Windo
		ws Firewall: Public:
		Logging: Log dropped
		packets
Set 'Windows Firewall: Public:	Level 1 - Domain	Audit:
Logging: Log successful	Controller	HKEY LOCAL MAC
connections' to 'Yes'	Level 1 - Member Server	HINE\Software\Policies\
		Microsoft/WindowsFire
		wall\PublicProfile\Loggi
		ng\LogSuccessfulConne
		ctions
		cuons
		Dama listiana Commeter
		Remediation: Computer
		Settings\Security
		Settings\Windows
		Firewall with Advanced
		Security\Windows
		Firewall with Advanced
		Security\Windows
		Firewall
		Properties\Public
		Profile\Logging\Windo
		ws Firewall: Public:
		Logging: Log successful
		connections
Set 'Audit Credential	Level 1 - Domain	To implement the
Validation' to 'Success and	Controller	recommended
Failure'	Level 1 - Member Server	configuration state set
		the following Group
		the following Oroup

		Policy setting to Success	
		and Failure.	
		Computer	
		Configuration	
		Settings/Security	
		Settings\Advanced	
		Audit Policy	
		Configuration Audit	
		Foncies Account	
		Logon\Audit Policy:	
		Account Logon:	
		Credential Validation	
	Level I - Domain	The recommended state	
Set 'Audit Computer Account	Controller	for this setting is:	
Management' to 'Success and	Level 1 - Member Server	Success and Failure.	
Failure'			
		Remediation: Computer	
		Configuration\Windows	
		Settings\Security	
		Settings\Advanced	
		Audit Policy	
		Configuration\Audit	
		Policies\Account	
		Management\Audit	
		Policy: Account	
		Management: Computer	
		Account Management	
Set 'Audit Distribution Group	Level 1 - Domain	The recommended state	
Management' to 'Success and	Controller	for this setting is:	
Failure'		Success and Failure.	
		Remediation: Computer	
		Configuration Windows	
		Settings/Security	
		Settings Advanced	
		Audit Policy	
		Configuration Audit	
		Policies Account	
		Management Audit	
		Delievy Account	
		Foncy: Account	
		Nanagement:	
		Distribution Group	
		Ivianagement	
Set 'Audit Other Account	Level 1 - Domain	The recommended state	
Management Events' to 'Success	Controller	for this setting is	
and Failure'	Level 1 - Member Server	Success and Failure	
		Success and Fantice.	
		Remediation:	

		To implement the recommended configuration state, set the following Group Policy setting to Success and Failure.	
		Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\Audit Policy: Account Management: Other Account Management Events	
Set 'Audit Security Group Management' to 'Success and Failure'	Level 1 - Domain Controller Level 1 - Member Server	The recommended state for this setting is: Success and Failure. Remediation: Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\Audit Policy: Account Management: Security Group Management	
Set 'Audit User Account Management' to 'Success and Failure'	Level 1 - Domain Controller Level 1 - Member Server	Remediation: To implement the recommended configuration state, set the following Group Policy setting to Success and Failure. Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\Audit Policy: Account	

		Management: User
		Account Management
Set 'Audit Process Creation' to	Level 1 - Domain	Remediation:
'Success'	Controller	
Success	Level 1 - Member Server	To implement the
		recommended
		configuration state set
		the following Group
		Policy setting to
		Success
		Success.
		Computer
		Configuration
		Settings/Security
		Settings Advanced
		Audit Policy
		Configuration
		Policies\Detailed
		Tracking Audit Policy:
		Detailed Tracking
		Process Creation
Set 'Audit Directory Service	Level 1 - Domain	Remediation:
Access' to 'Success and Failure'	Controller	
	Controller	To implement the
		recommended
		configuration state, set
		the following Group
		Policy setting to Success
		and Failure.
		Computer
		Configuration\Windows
		Settings\Security
		Settings\Advanced
		Audit Policy
		Configuration\Audit
		Policies\DS
		Access\Audit Policy: DS
		Access: Directory
		Service Access