Configure Group Policy for PCI with screenshot

Task 1: Ensure the system is configured to disable automatic administrator login.

🗐 Group Policy Management Editor - O × Ele Action View Help 🦛 🔿 🖄 📅 🐁 📋 🗰 🕰 🍙 📓 🖬 🙆 😏 🔸 Workstations [WSUS.CONTOSO.LC Registry 🖃 褬 Computer Configuration 15 Policies
 Preferences 🖃 🚞 Windows Settings Name Order Action Hive ۲ Processing % Environment There are no items to show in this view. 😽 Files Folders 🗉 💣 Registry Retwork Shares Shortcuts 1 General Settings 🖃 💰 User Configuration Policies 🖲 🚞 Preferences 2 Description No policies selected Preferences / Extended > Standard / 4 Registry

Create Group Policy Preference disable auto-logon. Here are example screenshots

In the Menu click on Action > New > Registry Item

Action	Undate	
Hive:	HKEY_LOCAL_MACHINE	_
Key Path:		
Value name		
De <u>f</u> ault		
Value konst		
value type:	JREG_SZ	<u> </u>
Value data:	1	

1	Group Policy Management Editor
File Action View Help	📾 🗟 🛃 🚮 🙆 💊 🔸 t 🤉
 Default Domain Policy [Computer Configuration Policies Preferences Windows Settings Environment 	AutoAdminLogon Properties
Files Folders Ini Files Registry Network Shares Shortcuts Control Panel Setting	Hive: HKEY_LOCAL_MACHINE Key Path: SOFTWARE\Microsoft\Windows NT\CurrentVel Value name Default AutoAdminLogon
 ⊿ K User Configuration ▷ ○ Policies ▷ ○ Preferences 	Value type: REG_SZ v Value data: 0
< III >	OK Cancel Apply Help

Enable AutoLogon

Key: HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon Value: AutoAdminLogon (REG_SZ) Data: 1 (Enabled) or 0 (Disable)

<u>F</u> ile	Edit	View I	F <u>a</u> vorites	<u>H</u> elp				
			Þ - 🍌	SystemRestore	^	Name	Туре	Data
				Terminal Server Time Zones Tracing UnattendSettings WbemPerf Windows Windows Activation Te Winlogon Winsat		 (Default) AutoAdminLogon AutoRestartShell Background CachedLogonsC DebugServerCo DefaultDomain DefaultPassword 	REG_SZ REG_DWORD REG_SZ REG_SZ REG_SZ REG_SZ REG_SZ REG_SZ REG_SZ REG_SZ	(value not set) 1 0x00000001 (1) 0 0 0 10 00 CONTOSO S3creet
			Window Window Window Window	WUDF ws Photo Viewer ws Portable Devices ws Script Host ws Search		DisableCAD ForceUnlockLog b LegalNoticeCap b LegalNoticeText PasswordExpirv	REG_DWORD REG_DWORD REG_SZ REG_SZ REG_DWORD	0x00000000 (0) 0x000000000 (0) 0x000000005 (5)
		→	Wisp Worksp Wwans ozillaPlu DBC	paces ivc gins		ab PowerdownAfte ab PreCreateKnow ab ReportBootOk ab scremoveoption ab Shell	REG_SZ REG_SZ REG_SZ REG_SZ REG_SZ	0 {A520A1A4-178 1 0 explorer eye
1		Or Po Re So	acle olicies gistered onic	Applications	4 III	BhutdownFlags BhutdownWitho ButdownWitho	REG_DWORD REG_SZ REG_SZ	0x00000027 (39) 0 C:\Windows\sy

Task 2: The built in Administrator and Guest accounts should be renamed to something other an Administrator or Guest or disabled.

To disable local administrative accounts throughout the domain I would use group policy to accomplish the task. The GPO can be created by using the Computer Policy | Windows Settings | Security Settings | Local policies | Security Options and then using the Accounts:Administrator account status setting. If this setting is GPO is linked to the domain level it can effective disable all of the local admin accounts.



Task 3: The system screen saver settings should be configured to lock the screen as required by organizational or regulatory policy.

You can enable Group Policy settings that control whether users use screen savers and whether they can change screen saver properties. Table 8.8 lists and describes each Group Policy setting. Other Group Policy settings you enforce can affect screen saver Group Policy settings. For additional information, right-click the Group Policy setting, click Properties , and then click the Explain tab, or refer to the Group Policy Reference on the Windows 2000 Resource Kit companion CD. The Group Policy settings listed in Table 8.8 are located in the Group Policy snap-in under Local Computer Policy\User Configuration\Administrative Templates\Control Panel\ Personalization.



Task 4: The Application, System, and Security Event log files should have ACLs set as follows: Administrators – Read and Execute. System – Full Control.



For DC, I applied Above steps are enough. For other computers, we may apply Group policy.

Use the Computer's Local Group Policy to Set Your Application and System Log Security

1. Click **Start**, click **Run**, type gpedit.msc, and then click **OK**.

2. In the Group Policy editor, expand **Windows Setting**, expand **Security Settings**, expand **Local Policies**, and then expand **Security Options**.

3. Double-click **Event log: Application log SDDL**, type the SDDL string that you want for the log security, and then click **OK**.

4. Double-click **Event log: System log SDDL**, type the SDDL string that you want for the log security, and then click

OK.

Use Group Policy to Set Your Application and System Log Security for a Domain, Site, or Organizational Unit in Active Directory

Important: To view the group policy settings that are described in this article in the Group Policy editor, first complete the following steps, and then continue to the "Use Group Policy to Set Your Application and System Log Security" section:

1. Use a text editor such as Notepad to open the Sceregyl.inf in the %Windir%\Inf folder.

2. Add the following lines to the [Register Registry Values] section:

 $MACHINE \ System \ Current Control Set \ Services \ Event log \ Application \ Custom SD, 1, \ Mapped Services \ MSD\%, 2$

 $MACHINE \ System \ Current Control Set \ Services \ Event log \ Security \ Custom SD, 1, \ Sec \ Custom SD, 2 \ Sec \$

 $MACHINE \ System \ Current Control Set \ Services \ Event log \ System \ Custom SD, 1, \ SysCustom SD, 3, \ SysCustom \ SD, 2, \ SysCustom \ SD, 3, \ SD, 3,$

MACHINE\System\CurrentControlSet\Services\Eventlog\Directory Service\CustomSD,1,%DSCustomSD%,2 MACHINE\System\CurrentControlSet\Services\Eventlog\DNS Server\CustomSD,1,%DNSCustomSD%,2 MACHINE\System\CurrentControlSet\Services\Eventlog\File Replication Service\CustomSD,1,%FRSCustomSD%,2

3. Add the following lines to the [Strings] section:

AppCustomSD="Eventlog: Security descriptor for Application event log"

SecCustomSD="Eventlog: Security descriptor for Security event log"

SysCustomSD="Eventlog: Security descriptor for System event log"

DSCustomSD="Eventlog: Security descriptor for Directory Service event log" DNSCustomSD="Eventlog: Security descriptor for DNS Server event log" FRSCustomSD="Eventlog: Security descriptor for File Replication Service event log"

4. Save the changes you made to the Sceregvl.inf file, and then run the regsvr32 scecli.dll command.

5. Start Gpedit.msc, and then double-click the following branches to expand them:

Computer Configuration Windows Settings Security Settings Local Policies Security Options

6. View the right panel to find the new "Eventlog" settings.

Use Group Policy to Set Your Application and System Log Security

1. In the Active Directory Sites and Services snap-in or the Active Directory Users and Computers snap-in, right-click the object for which you want to set the policy, and then click **Properties**.

2. Click the Group Policy tab.

3. If you must create a new policy, click **New**, and then define the policy's name. Otherwise, go to step 5.

4. Select the policy that you want, and then click **Edit**.

The Local Group Policy MMC snap-in appears.

5. Expand Computer Configuration, expand Windows Settings, expand Security Settings, expand Local Policies, and then click Security Options. 6. Double-click **Event log: Application log SDDL**, type the SDDL string that you want for the log security, and then click **OK**.

7. Double-click **Event log: System log SDDL**, type the SDDL string that you want for the log security, and then click **OK**.

Task 5: Each partition/drive should be set to audit "Failures" for the Everyone group at a minimum. Computer Configuration>Policies>Windows settings>Advanced Audit Policy Configuration>Object Access>Audit File System.

			() - () - () - () - ()
Action View Help Image: Computer Configuration Image: Policies Policies Image: Software Settings Image:	 Subcategory Audit Applica Audit Certifica Audit Certifica Audit Detailed Audit File Sha Audit File Sha Audit File System Audit Central 	tion Generated ation Services 4 File Share re tem g Platform Connection g Platform Packet Drop Manipulation Dbject Object Object Access Events / able Storage Access Policy Staging	Audit Events Not Configured Not Configured
 Network List Manager Policies Wireless Network (IEEE 802.11) Policies Public Key Policies Software Restriction Policies Network Access Protection Application Control Policies IP Security Policies on Active Directory (C 	~		
m	1	m	

A Forest: core.kosmek.com Audit File System P	roperties	Group	Policy Management Editor	_ 0 X
Audit File System P Policy Belain Audit File System Configue the following audit events: Success Falure	roperties	Group New Help Normal Services System Services System Services System Services System Services Windows Firewall with Advanced Se Software Restriction Policies Deltaide Policies Windows Firewall with Advanced Se Windows Firewall with Advanced Se Windows Access Protection Deltaide Policies Deltaide Policies Deltaide Tracking Disc Cacess Disc Change Disc Change Disc Vintege Use	Policy Management Editor	Audit Events Not Configured Not Configured
-		b 🗿 Global Object Access Auditir		

Task 6: Configure the system to disallow guest access to the Event logs.

Computer configuration>Policies>Windows settings> Security settings>Local Policy>Security options>

Links Dipplay links in the Deplay links in the The following stee Location Image: CCN - restrict eventlog access[Image: CCN - restrict eventlog access[Image: CCN - restrict eventlog access[Image: CCN - restrict eventlog access[Image: CCN - restrict eventlog access[Image: CCN - restrict eventlog access[Image: CCN - restrict eventlog access[Image: CCN - restrict eventlog access[Image: CCN - restrict eventlog access[Image: CCN - restrict eventlog access[Image: CCN - restrict eventlog access[Image: CCN - restrict eventlog access[Image: CCN - restrict eventlog access[Image: CCN - restrict eventlog access[Image: CCN - restrict eventlog access[Image: CCN - restrict eventlog access[Image: CCN - restrict eventlog access[Image: CCN - restrict eventlog access[Image: CCN - restrict eventlog access[Image: CCN - restrict eventlog access[Image: CCN - restrict eventlog access[Image: CCN - restrict eventlog access[Image: CCN - restrict eventlog access[Image: CCN - restrict eventlog access[Image: CCN - restrict eventlog accessing application log Image: CCN - restrict eventlog accessing application log Image: CCN - restrict eventlog accessing application log Image: CCN - restrict foroups Imag	Scope Details	g	Group Policy Management Editor	_ 0 X
Add	Scope Details Details Details Details Depays Inks in the The following sites Location Location Security Filterir The settings in the Name Authenticate	File Action View Help	Group Policy Management Editor Policy Maximum application log size Maximum security log size Maximum system log size Prevent local guests group from accessing application log Prevent local guests group from accessing system log Retain application log Retain security log Retain system log Retain system log Retention method for application log Retention method for system log Retention method for system log Retention method for system log	Policy Setting Not Defined Not Defined Enabled Enabled Enabled Not Defined Not Defined Not Defined Not Defined Not Defined Not Defined
	Add	Windows Firewall with Windows Firewall with Network List Manager Wireless Network (IEE Public Key Policies V	۲ 🖬	>

Task 7: The HKEY_LOCAL_MACHINE\SOFTWARE and HKEY_LOCAL_MACHINE\SYEM registry hives should have auditing set to record "Failures" for the everyone group at a minimum.





Task 8: The system event log size, and retention policy should be set to comply with organizational or regulatory requirements.

Microsoft has verified that the practical size limit for all event logs combined is around 300 megabytes (MB) on most servers. On Windows XP, member servers, and stand-alone servers, the combined size of the application, security, and system event logs should not exceed 300 MB. On domain controllers, the combined size of these three logs — plus the Directory Service, File Replication Service, and DNS Server logs — should not exceed 300 MB.

3. Do I do all servers and workstations? if so, I assume I will work on workstations only in the evening. Right?

Computer configuration>Policies>Windows settings>Security Settings>Event log.

le Action View Help	Policy Maximum application log size Maximum security log size Maximum system log size Prevent local guests group from accessing applica Prevent local guests group from accessing security Prevent local guests group from accessing system Retain application log Retain security log Retain system log Retention method for application log Retention method for security log Retention method for system log Retention method for system log	Policy Setting 294912 kilobytes 294912 kilobytes 294912 kilobytes 294912 kilobytes tion log Enabled log Enabled Not Defined Not Defined Not Defined Not Defined Not Defined
Windows Firewall with Adva Network List Manager Polici		

Task 9: The system should be configured to override audit policy subcategory settings, in order to take advantage of the more precise auditing features included in Windows Vista or later.

Resolution:

Disable the policy setting by using Group Policy Object Editor

Verify that the policy setting was enabled by using Group Policy, and then disable the policy setting by using Group Policy Object Editor. To do this, follow these steps:

- 1. Verify that the "Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings" policy setting was enabled by using Group Policy. To do this, follow these steps:
 - 1. On the computer, click **Start**, point to **All Programs**, click **Accessories**, click **Run**, type rsop.msc in the **Open** box, and then click **OK**.
 - 2. Expand Computer Configuration, expand Windows Settings, expand Security Settings, expand Local Policies, and then click Security Options.
 - 3. Double-click Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings.
 - 4. Verify that the policy setting is set to **Enabled**, and then note the Group Policy object (GPO).
- 2. Disable the "Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings" policy setting in the GPO. To do this, follow these steps:
 - 1. In Group Policy Object Editor, open the GPO.
 - Expand Computer Configuration, expand Windows Settings, expand Security Settings, expand Local Policies, and then click Security Options.
 - 3. Double-click Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings.
 - 4. Click **Disabled**, and then click **OK**.

3. Restart the computer or computers.



Refer to

This may be of help

https://support.microsoft.com/en-us/help/921468/security-auditing-settings-are-not-applied-towindows-vista-based-and

Don't take this one:

Best practices
₂

•Leave the setting enabled. This provides the ability to audit events at the category level without revising a policy.

Location **?**

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

Default values?

The following table lists the actual and effective default values for this policy. Default values are also listed on the policy's property page.+

Server type or GPO

Default value

Default Domain Policy Not defined Default Domain Controller Policy Not defined Stand-Alone Server Default Settings Enabled DC Effective Default Settings Enabled Member Server Effective Default Settings Enabled Client Computer Effective Default Settings Enabled

Reference: Audit Force **audit policy subcategory settings** (Windows Vista or later ...

Apr 19, 2017 ... Describes the best practices, location, values, and security considerations for the Audit Force **audit policy subcategory settings** (Windows Vista or later) to **override** audit policy category settings security policy setting. docs.microsoft.com

https://docs.microsoft.com/...policy-settings/audit-force-audit-policy- subcategory-settings-to-override

Task 10: User Account Privilege Controls – location: Computer Configuration>Polices>Windows settigns>Security Settings>Local policies>User rights assignments. Ensure the following User Rights are assigned:

Before

Access this computer from the network Properties
Access this computer from the network
Define these policy settings:
ASPNET NUSR_KOSMEK-SERVER NWAM_KOSMEK-SERVER
Pre-Windows 2000 Compatible Access
Add User or Group Remove
Modifying this setting may affect compatibility with clients, services, and applications. For more information, see <u>Access this computer from the network</u> . (Q823659)
OK Cancel Apply

After

ecurity Policy Setting	Explain
Access this	s computer from the network
Define these polic	v settings:
Authenticated Users VASPNET UUSR_KOSM UWAM_KOSM domain admins	IEK-SERVER MEK-SERVER
ENTERPRISE DOM	AIN CONTROLLERS
ENTERPRISE DOM	AIN CONTROLLERS

Add workstations to domain – Administrators Before

Add workst	Explain ations to domain
Define these polic Authenticated Users	y settings:
Add User or Gro	up Remove

After

becamy roscy bearing	Explain
Add workst	ations to domain
Define these policy	v settings:

Adjust memory quotas for a process – Administrators, Local Service, Network Service

Before

	Explain
Adjust men	nory quotas for a process
Define these polic	cy settings:
\IWAM_I	SERVER
Additions of Con	
Add User or Gro	Pemove
Add User or Gro	pup
Add User or Gro	Bemove

After

Adjust	ting Explain memory quota	s for a process	
Define these p administrators local service network service	policy settings:		
	r Group	Remove	
Add User or			

Allow log on locally – Administrators Before

Security Policy Setting	Explain	
Allow log or	n locally	
Define these polic	y settings:	
Additionary	Barran	
ACC LISELOUISES	up nemove	

After

Allow log or	n locally	
Define these polic	y settings:	
domain admins		
Add User or Gro	Remove	
Add User or Gro	Remove setting may affect compatibility with clients, service	s,
Add User or Gro Modifying this and applicatio For more infor	Remove setting may affect compatibility with clients, service ons. mation, see <u>Allow log on locally</u> . (Q823659)	s,

Allow log on through Terminal Services – Administrators Before

Allow log or	through Re	emote Desktoj	Services	
Define these policy	y settings:			
10 A	A \$25,59095	-		
				I
Add User or Gra	(m)	Remove	1	
Add User or Gro	up not compati	Remove ble with comp	uters running W	indows
Add User or Grou This setting is 2000 Service containing this	not compati Pack 1 or e. s setting only	Remove ble with comp artier. Apply G v to computers	uters running W roup Policy obje running a later	indows acts version of
Add User or Gro This setting is 2000 Service containing this the operating a	up not compati Pack 1 or e. s setting only system.	Remove ble with comp arlier. Apply G v to computers	uters running W roup Policy obje running a later	indows ects version of

After

Allow log or	hrough Remote Desktop Services	
Define these policy	settings:	
dministrators		
		.17
Add User or Gro	Remove	
This setting is 2000 Service containing this the operating s	ot compatible with computers running V ack 1 or earlier. Apply Group Policy ob etting only to computers running a later stem.	Vindows jects version of

Backup files and directories – Administrators Before

becunity Folicy Setting	Explain
Back up file	es and directories
Define these policy	/ settings:

After

Secondy Policy Setting	Explain
Back up file	es and directories
Define these policy	y settings:
administrators	

Bypass traverse checking – Administrators, Authenticated Users, Local Service, Network Service

Before

Security Policy Setting	Explain	
Bypass trav	erse checking	
Define these policy	r settings:	
0		
		1.00
a		
Add User or Gro	upRemove	
Modifying this	setting may affect compatibility with clier	nts, services,



Security Policy Setting	Explain
Bypass trav	erse checking
Administrators Authenticated Users LOCAL SERVICE NETWORK SERVIC	E

Change the system time – Administrators, Local Service Before

Change the	System time	
Define these policy	/ settings:	
Add User or Gro	up	
Add User or Gro	up Remove	

After

Change the	system time	
Define these policy	y settings:	
Administrators LOCAL SERVICE		
		ų. R
Add User or Gro	up	10 20
Add User or Gro	up	
Add User or Gro	up	

Change the time zone – Administrators, Local Service Before

Change the	time zone			
Define these policy	y settings:			
		110000000000000000000000000000000000000		
Add User or Gro	up	Remove	1	

After

Change the	Explain time zone		 	
 Define these policy 	/ settings:			
Administrators LOCAL SERVICE	8 82		 	
Add User or Grou	ир	Remove		

Create a pagefile – Administrators No settings before. Now added admin.

Create a token object – (None) No change

Create global objects – Administrators, Service, Local Service, Network Service No settings before. Now added them accordingly.

Create permanent shared objects – (None) No change

Create symbolic link – Administrators

Task 11: Networking Security

Ensure the system is configured to enable user notification is a web based program attempts to install software.

Group Policy location: Computer Configuration >> Administrative Templates >> Windows Components >> Windows Installer >> "Prevent Internet Explorer security prompt for Windows Installer scripts" to "Not Configured" or "Disabled". No change

Network and Dial-up Connections folders in

Computer Configuration\Administrative Templates\Network\Network and Dial-up Connections and User Configuration\Administrative Templates\Network\Network and Dial-up Connections. No change.

Ensure that the system is preserving zone information for attachments, to enable Windows to determine the risk of file attachments.

Information about the Attachment Manager in Microsoft Windows

Jun 26, 2017 ... By not **preserving** the **zone information**, Windows cannot make appropriate risks assessments. If you enable this policy setting, Windows does not mark file **attachments** by using their **zone information**. If you disable this policy setting, Windows marks file **attachments** by using their **zone information**. If you do ... support.microsoft.com

https://support.microsoft.com/.../information-about-the-attachment-manager- inmicrosoft-windows

Ensure the system is configured to hide the ability for users to manually remove the zone information of file attachments.

If the following registry value doesn't exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_Current_User

Subkey: \Software\Microsoft\Windows\CurrentVersion\Policies\Attachments\

Value Name: HideZoneInfoOnProperties

Type: REG_DWORD

Value: 1

Fix Text (F-13607r1_fix)

Configure the policy value for User Configuration -> Administrative Templates -> Windows Components -> Attachment Manager -> "Hide mechanisms to remove zone information" to "Enabled".

ile Action View Help	The state of the s		
🔿 🖄 🖬 🗟 🖬 🔻			
🔺 📑 Windows Components 🛛 🔿	Setting	State	Comment
Add features to Windows 8	E Notify antivirus programs when opening attachments	Not configured	No
App runtime	E Trust logic for file attachments	Not configured	No
Application Compatibility	E Do not preserve zone information in file attachments	Not configured	No
Attachment Manager	Hide mechanisms to remove zone information	Enabled	No
AutoPlay Policies	E Default risk level for file attachments	Not configured	No
Credential User Interface	E Inclusion list for high risk file types	Not configured	No
Desktop Gadgets	E Inclusion list for low file types	Not configured	No
Desktop Window Manager Digital Locker	E Inclusion list for moderate risk file types	Not configured	No

Unless a documented need exists, ensure that Windows Peer to Peer Networking Services are disabled, as well as the ability to create a Network Bridge.

In the Group Policy window please navigate to Computer Configuration -> Administrative Templates -> Network -> Microsoft Peer-to-Peer Networking Services and open Turn off Microsoft Peer-to-Peer Networking Services. Note: If you enable this setting, peer-to-peer protocols will be turned off.

g 🖉	🗸 🖶 🛱 LeigMein - RentotinSeadon	× =	_
File Action View Help			
🗢 🔿 🙇 📷 🔂 📾 🐨			
- Removed from Default Domain Contro	Setting	State	Comment
a 🙀 Computer Configuration	Peer Name Resolution Protocol		
a Dolicies	Disable password strength validation for Peer Grouping	Not configured	No
Software Settings	Turn off Microsoft Peer-to-Peer Networking Services	Enabled	No
Windows Settings			
A 🧮 Administrative Templates: Policy c			
D Control Panel			
a 🔛 Network			
Background Intelligent Trai			
BranchCache			
DirectAccess Client Experie			
DNS Client			
Hotspot Authentication			
🛄 Lanman Server 🖉			
Link-Layer Topology Disco			
Microsoft Peer-to-Peer Net			

The system should be configured to prevent the downloading of attachments or enclosures via RSS feeds.

Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> RSS Feeds "Turn off downloading of enclosures" to "Enabled". – not found. User configuration>Policies>Administrative Templates Policies>Windows Components>RSS Feed>Prevent downloading enclosures.

4 🗾 Windows Components 🛛 🔿	Setting	State	Comment
Add features to Windows 8	Turn on Basic feed authentication over HTTP	Not configured	No
🔛 App runtime	Turn off background synchronization for feeds and Web Slic	Not configured	No
Application Compatibility	Prevent downloading of enclosures	Enabled	No
Attachment Manager	Prevent subscribing to or deleting a feed or a Web Slice	Not configured	No
AutoPlay Policies	Prevent automatic discovery of feeds and Web Slices	Not configured	No
Credential User Interface	Prevent access to feed list	Not configured	No
Desktop Gadgets			
Desktop Window Manager			
Digital Locker			
Edge UI			
File Explorer			
File Revocation			
IME			
Instant Search			
Internet Explorer			
Cocation and Sensors			
Microsoft Management Co =			
NetMeeting			
Network Projector			
Carl Network Sharing			
Presentation Settings			
Remote Desktop Services			
RSS Feeds			

Configure the system to prevent the sending of unencrypted passwords to third party SMB servers.

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

Microsoft network client: Send unencrypted password to connect to third-party SMB servers to Disabled

Configure the system to disallow anonymous remote registry access. Using the Registry Editor, navigate to the following key:

MACHINE/System/CurrentControlSet/Control/SecurePipeServers/Winreg

If the key does not exist, then this is a finding. If the permissions are not at least as restrictive as those below, then this is a finding.

Administrators - Full Backup Operators - Read(QENR) Local Service - Read



Ensure the LanMan authentication level is set to at least: "Send NTLMv2 response only\refuse LM". Network security: LAN Manager authentication level Location?

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

	- H A .	all kosmek-ad3	et Editor - 8
File Action View Help	Logmoin - K	emole Session	
(+ +) 2 🗊 🗙 🖬 🗟 🖬		-	
- Removed from Default Domain Controlle	Policy	-	Policy
4 👫 Computer Configuration			
⊿ 🧾 Policies	Network sec	curity: LAN Manager authen	tication lev
Software Settings	County Pole	Setting Transl	
a 🔛 Windows Settings	Security Policy	Explain	
Name Resolution Policy	illin Ne	etwork security: LAN Manager authent	ication level
Scripts (Startup/Shutdown)			
Deployed Printers			
A Security Settings	 Define this 	is policy setting	
Account Policies	Send N	TLM response only	¥
⊿			
Audit Policy	Mode	fying this setting may affect compatibil	ity with clients, services,
User Rights Assignment	For m	applications, nore information, see Network security	LAN Manager
J Security Options	authe	entication level. (Q823659)	

The Guests account group should be denied the ability to login to the machine remotely.



The system should be configured to perform SMB packet signing and encryption wherever possible

You can configure this method by enabling the Microsoft network client: Digitally sign communications (always) and the Microsoft network server: Digitally sign communications (always) options

Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options.



Ensure the system is configured to require secure RPC connections

Computer Configuration \ <policies> \ Administrative Templates \ System \ Remote Procedure Call

Restrictions for unauthenticated RPC clients RPC endpoint mapper client authentication

⊿ 🛗 System	Setting		State	Comment	
Access-Denied Assistance Audit Process Creation Credentials Delegation Device Installation Disk NV Cache	Enable RPC Endpoint Mapper Client Ignore Delegation Failure Maintain RPC Troubleshooting State Propagate extended error informatio Restrict Unauthenticated RPC clients	Authentication Information n	Not configured Not configured Not configured Not configured Not configured	No No No No No	
Disk Quotas Distributed COM		Restrict Unauthe	enticated RPC clients		
Driver Installation Early Launch Antimalware File Classification Infrastruc	Restrict Unauthenticated RPC clien	ts	Previous Setting Next Settin	ng	
 File Share Shadow Copy Pri Filesystem Folder Redirection 	Not Configured Comment: Enabled				
Group Policy Group Policy Gilden Internet Communication N Gilden ISCSI Gilden KDC Gilden ISCSI	 Disabled Supported on: 	In: At least Windows XP Professional with SP2			
 Kerberos Locale Services Logon 	Options:	Hel	p:		
 Net Logon Power Management 	RPC Runtime Unauthenticated Client Re Apply:	estriction to	is policy setting controls how the RPC serve authenticated RPC clients connecting to RP	er runtime handles PC servers.	
Remote Assistance Remote Assistance Remote Procedure Call Removable Storage Access Scripts Server Manager Shutdown Shutdown System Restore Troubleshooting and Diagr	Authenticated without exceptions	✓ Thi envices the environment of the envisionment of the environment of the environment of the environme	is policy setting impacts all RPC application vironment this policy setting should be usen n impact a wide range of functionality inclu occessing itself. Reverting a change to this p juire manual intervention on each affected licy setting should never be applied to a doi you disable this policy setting, the RPC serve ue of "Authenticated" on Windows Client, a one" on Windows Server versions that supp ting. You do not configure this policy setting, it re e RPC server runtime will behave as though the the value of "Authenticated" used for Windows Server is policy setting.	is, In a domain d with caution as it iding group policy olicy setting can machine. This main controller. er runtime uses the and the value of ort this policy in dows emains disabled.	

The system should have Microsoft Windows Defender SpyNet reporting disabled.

Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Windows Defender "Configure Microsoft Spynet Reporting" to "Disabled".

N/A. This is DC.

The system should have Kerberos configured in the following manner: Maximum lifetime for service ticket – 600 minutes or fewer. Maximum lifetime for user ticket – 10 hours or less. Maximum lifetime for user ticket renewal – 7 days or fewer. Maximum tolerance for computer clock synchronization – 5 minutes or less

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



Configure the system to ignore NetBIOS name release requests from all systems except WINS servers. Configure the policy value for Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Security Options -> "MSS: (NoNameReleaseOnDemand) Allow computer to ignore NetBIOS name release requests except from WINS servers" to "Enabled".

I don't see "MSS: (NoNameReleaseOnDemand) Allow computer to ignore NetBIOS name release requests except from WINS servers" because this reason:

The mystery of the missing 'MSS:' setting on Windows 2008

Nov 22, 2010 ... For this purpose we created an .adm file, which can be loaded into the **Group Policy** editor as a Classic Administrative template. All the MSS settings ... Setting: MSS: (NoNameReleaseOnDemand) Allow the computer to **ignore** Description: **NetBIOS name release requests** except from WINS servers. Defines ... stories.schubergphilis.com

https://stories.schubergphilis.com/the-mistery-of-the-missing-mss-setting-on- windows-2008-6279d2745f0a

If the value for "MSS: (NoNameReleaseOnDemand) Allow computer to ignore NetBIOS name release requests except from WINS servers" is not set to "Enabled", then this is a finding.

The policy referenced configures the following registry value:

Registry Hive: HKEY_LOCAL_MACHINE Registry Path: \System\CurrentControlSet\Services\Netbt\Parameters\

Value Name: NoNameReleaseOnDemand

Value Type: REG_DWORD Value: 1

Note: The NetBIOS name for the system will no longer appear under 'My Network Places'.



The system should be configured to disable AutoRun for all drives and removable media. Under Computer Configuration, expand Administrative Templates, expand Windows Components, and then click Autoplay Policies.

🛛 🧮 Windows Components 👘 🔿	Setting		State	Comm	nent
ActiveX Installer Service	E Disallow Autoplay for non-volume devi	ces	Not configure	d No	,
Add features to Windows 8	Prevent AutoPlay from remembering us	ser choices.	Not configure	d No	1
App Package Deployment	E Set the default behavior for AutoRun		Not configure	d No	,
App runtime Application Compatibility	Turn off Autoplay		Not configure	d No	1
AutoPlay Policies	÷	Turn off Au	itoplay		
BitLocker Drive Encryption Credential User Interface Desktop Gadgets	Turn off Autoplay		Previous Setting	Next Setting	
Desktop Window Manager	O Not Configured Comment:				
Device and Driver Compati Digital Locker	 Enabled 				
🛗 Edge UI	O Disabled				
 Event Forwarding Event Log Service Event Viewer 	Supported on:	At least Windows 2000			
 ☐ Family Safety ↓ ☐ File Explorer 	Options:	Help:			

Anonymous SID/Name translation should be disabled.

Location: Computer Configuration/Windows Settings/Security Settings/Local Policies/Security Options

Network access: Allow anonymous SID/Name translation

- Removed from Default Domain Controlle	Policy	Policy Setting
 Kenoved from Default Domain Controlle Computer Configuration Policies Software Settings Windows Settings Name Resolution Policy Scripts (Startup/Shutdown) Below Deployed Printers Security Settings Account Policies Local Policies Local Policy Security Options Event Log Kenstricted Groups System Services Registry 	 Policy Interactive logon: Machine inactivity limit Interactive logon: Message text for users attempting to log on Interactive logon: Message title for users attempting to log on Interactive logon: Number of previous logons to cache (in case domain controller i Interactive logon: Prompt user to change password before expiration Interactive logon: Require Domain Controller authentication to unlock workstation Interactive logon: Smart card removal behavior Microsoft network client: Digitally sign communications (always) Microsoft network client: Send unencrypted password to third-party SM8 servers Microsoft network server: Amount of idle time required before suspending session Microsoft network server: Digitally sign communications (always) Microsoft network server: Digitally sign communications (if client agrees) Microsoft network server: Digitally sign communications (if client agrees) Microsoft network server: Digitally sign communications (if client agrees) Microsoft network server: Digitally sign communications (if client agrees) Microsoft network server: Disconnect clients when logon hours expire 	Policy Setting Not Defined Not Defined Enabled Not Defined Enabled Not Defined Not Defined Not Defined Not Defined Not Defined Not Defined
File System Wired Network (IEEE 802.3) Po	Microsoft network server: Server SPN target name validation level Network access: Allow anonymous SID/Name translation	Not Defined Disabled
	10500-00 part of the second	Contraction of the

Anonymous access to named pipes should be limited to the following: COMNAP, COMNODE, SQL\QUERY, SPOOLSS, LLSRPC, BROWSER, NETLOGON, Lsarpc, samr".

Location: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options Enable: Network access: Restrict anonymous access to Named Pipes and Shares

- Removed from Default Domain Controlle	Policy	Policy Setting
a 🙀 Computer Configuration	B Microsoft network server: Digitally sign communications (if client agrees)	Not Defined
⊿ 🧮 Policies	Alicrosoft network server: Disconnect clients when logon hours expire	Not Defined
Software Settings Windows Settings	C Microsoft network server: Server SPN target name validation level	Not Defined
Name Resolution Policy	Network access: Allow anonymous SiD/Name translation Network access: Do not allow anonymous enumeration of SAM accounts	Not Defined
Scripts (Startup/Shutdown)	Network access: Do not allow anonymous enumeration of SAM accounts and shares	Not Defined
Security Settings	Network access: Do not allow storage of passwords and credentials for network aut	Not Defined
A Count Policies	Network access: Named Pipes that can be accessed anonymously	Not Defined
Audit Policy	Network access: Remotely accessible registry paths	Not Defined
User Rights Assignment Security Options	Network access: Remotely accessible registry paths and sub-paths	Enabled

If smartcard's in use, ensure that the system is configured to "lock the workstation", or "force logoff" on smartcard removal.

User Configuration\Policies\Administrative Templates\Control Panel\Personalization. The required settings are: 'Enable screen saver', 'Screen saver timeout', 'Force specific screen saver' (this is important because if the system has no screensaver configured this won't work) and finally 'Password protect the screensaver'.

This DC and don't use smartcard. N/A.

Remote accessible registry paths should be restricted to the following: System\CurrentControlSet\Control\ProductOptions System\CurrentControlSet\Control\Server Applications Software\Microsoft\Windows NT\CurrentVersion Location **?**

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



Network access: Remotely accessible registry paths and subpaths

No unapproved account should be able to "Debug programs" or have more than read access to Winlogon registry keys.

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

By default, members of the Administrators group have this right. No change.

7. The ACLs for all disabled services should be set as follows: Administrators – Full Control, System – Full Control, Interactive – Read. ???

8. Configure the system to disallow the storing of passwords using reversible encryption. Should not enabled



9. Ensure the system is configured to only allow Administrators to perform task scheduling. Domain controller: Allow server operators to schedule tasks

Location²

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

10. All file shares should have ACLs set to provide the minimum permissions possible to accounts which require access.

?Most share drives have everyone with full permission? ?

11. The system should be configured to require "Strong Session Keys", in order to prevent systems prior to Windows 2000 from authenticating or joining the domain.

Location: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options Network security: LAN Manager authentication level is set send NTLM response only



12. Configure the system to disallow the storage of credentials or .NET passports for network authentication.

Enable Network access: Do not allow storage of passwords and credentials for network authentication Location: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options

⊿ 🧮 Policies	~	Policy A	Policy Setting
 Software Settings Windows Settings Name Resolution Policy Scripts (Startup/Shutdown) Deployed Printers Security Settings Account Policies Audit Policy 		Microsoft network server: Attempt S4U2Self to obtain claim information Microsoft network server: Digitally sign communications (always) Microsoft network server: Digitally sign communications (if client agrees) Microsoft network server: Disconnect clients when logon hours expire Microsoft network server: Server SPN target name validation level Network access: Allow anonymous SID/Name translation Network access: Do not allow anonymous enumeration of SAM accounts Network access: Do not allow anonymous enumeration of SAM accounts	Not Defined Enabled Not Defined Not Defined Disabled Not Defined Not Defined
Ilser Rights Assignment		Network access: Do not allow storage of passwords and credentials for network aut	Enabled
Security Options		🐘 Network access: Let Everyone permissions apply to anonymous users	Not Defined

13. The "Sharing and security model for local accounts" setting should be set to "Classic – local accounts authenticate as themselves."

Network access: Sharing and security model for local accounts

Location Computer Configuration/Windows Settings/Security Settings/Local Policies/Security Options

?

a 🧾 Policies	~	Policy	Policy Setting
Software Settings		III Network access: Allow anonymous SID/Name translation	Disabled
🔺 🧮 Windows Settings	_	Network access: Do not allow anonymous enumeration of SAM accounts	Not Defined
Name Resolution Policy		Retwork access: Do not allow anonymous enumeration of SAM accounts and shares	Not Defined
Scripts (Startup/Shutdown)		In Network access: Do not allow storage of passwords and credentials for network aut	Enabled
Deployed Printers		Network access: Let Everyone permissions apply to anonymous users	Not Defined
Security Settings		In Network access: Named Pipes that can be accessed anonymously	Not Defined
Account Policies		Remotely access: Remotely accessible registry paths	System\CurrentControlSet\Con
		Retwork access: Remotely accessible registry paths and sub-paths	Not Defined
Here Pichts Accionment		III Network access; Restrict anonymous access to Named Pipes and Shares	Enabled
Security Options		Network access: Shares that can be accessed anonymously	Not Defined
Event log		Network access: Sharing and security model for local accounts	Classic - local users authenticat
P an evene bog		THE ALL ALL ALL ALL ALL ALL ALL ALL ALL AL	MIDE I

14. Ensure the system is configured to disallow the storage of the LanMangager password hash value.Enable Network security: Do not store LAN Manager hash value on next password change.In Group Policy, expand Computer Configuration, expand Windows Settings, expand Security Settings, expand Local Policies, and then click Security Options.

4 🧰 Policies	0	Policy A	Policy Setting
Software Settings Windows Settings		Network access: Remotely accessible registry paths Network access: Remotely accessible registry paths and sub-paths	System\CurrentControlSet\Con Not Defined
 Name Resolution Policy Scripts (Startup/Shutdown) 		Network access: Restrict anonymous access to Named Pipes and Shares	Enabled Not Defined
▷ Imployed Printers ▲ Security Settings		Network access; Sharing and security model for local accounts	Classic - local users authenticat Not Defined
Account Policies A Local Policies		Network security: Allow LocalSystem NULL session fallback Network security: Allow PKU2U authentication requests to this computer to use on	Not Defined Not Defined
Audit Policy User Rights Assignment	nt	Network security: Configure encryption types allowed for Kerberos	Not Defined
Security Options		Network security: Do not store LAN Manager hash value on next password change	Enabled

15. The system should be configured to use FIPS compliant algorithms for encryption, hashing, and signing.

Enable System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing Location Computer Configuration/Windows Settings/Security Settings/Local Policies/Security Options

a 📋 Policies 📃 🔿	Policy	Policy Setting
Software Settings	IN Network security: LAN Manager authentication level	Send NTLM response only
🔺 🚞 Windows Settings 📃	Network security: LDAP client signing requirements	Not Defined
Name Resolution Policy	Retwork security: Minimum session security for NTLM SSP based (including secur	Not Defined
Scripts (Startup/Shutdown)	Retwork security: Minimum session security for NTLM SSP based (including secur	Not Defined
Deployed Printers	Retwork security: Restrict NTLM: Add remote server exceptions for NTLM authenti	Not Defined
A Security Settings	Retwork security: Restrict NTLM: Add server exceptions in this domain	Not Defined
Account Policies	Network security: Restrict NTLM: Audit Incoming NTLM Traffic	Not Defined
⊿ Local Policies	Retwork security: Restrict NTLM: Audit NTLM authentication in this domain	Not Defined
Audit Policy	Network security: Restrict NTLM: Incoming NTLM traffic	Not Defined
Servite Options	IN Network security: Restrict NTLM: NTLM authentication in this domain	Not Defined
Event Log	Retwork security: Restrict NTLM: Outgoing NTLM traffic to remote servers	Not Defined
Restricted Groups	Recovery console: Allow automatic administrative logon	Not Defined
System Services	Recovery console: Allow floppy copy and access to all drives and all folders	Not Defined
N Benistry	Shutdown: Allow system to be shut down without having to log on	Not Defined
> A File System	Shutdown: Clear virtual memory pagefile	Not Defined
▷ In Wired Network (IEEE 802.3)	System cryptography: Force strong key protection for user keys stored on the com	Not Defined
Dindows Firewall with Adv	System cryptography: Use FIPS compliant algorithms for encryption, hashing, and	Enabled

16. Configure the setting "Default owner of objects created by the Administrators group" to read "Object Creator".

Windows Vista, Windows 7, Windows Server 2008 and Windows Server 2008 R2 do not support this setting any longer

A Group Policy setting is not available in the security policy settings ...

Describes a problem in which the "System **objects**: **Default owner** for **objects created** by members of the **Administrators group**" Group Policy setting is not available in the security policy settings list. A resolution is provided. support.microsoft.com

https://support.microsoft.com/.../a-group-policy-setting-is-not-available-in- the-security-policy-setting

17. Configure the system to "Require case insensitivity for non-Windows subsystems." Enable System objects: Require case insensitivity for non-Windows subsystems Location Computer Configuration/Windows Settings/Security Settings/Local Policies/Security Options

a 📔 Policies	^	Policy	Policy Setting
Software Settings		Retwork security: LAN Manager authentication level	Send NTLM response only
⊿ 🚞 Windows Settings	-	Retwork security: LDAP client signing requirements	Not Defined
Name Resolution Policy		📓 Network security: Minimum session security for NTLM SSP based (including secur	Not Defined
Scripts (Startup/Shutdown)		Retwork security: Minimum session security for NTLM SSP based (including secur	Not Defined
Deployed Printers		Restrict NTLM: Add remote server exceptions for NTLM authenti	Not Defined
A 🛅 Security Settings		Restrict NTLM: Add server exceptions in this domain	Not Defined
Account Policies		B Network security: Restrict NTLM: Audit Incoming NTLM Traffic	Not Defined
Local Policies		Retwork security: Restrict NTLM: Audit NTLM authentication in this domain	Not Defined
Audit Policy Licer Pichts Assignment		Retwork security: Restrict NTLM: Incoming NTLM traffic	Not Defined
Security Options		Retwork security: Restrict NTLM: NTLM authentication in this domain	Not Defined
N J Event Log		Restrict NTLM: Outgoing NTLM traffic to remote servers	Not Defined
Restricted Groups		Recovery console: Allow automatic administrative logon	Not Defined
System Services		Recovery console: Allow floppy copy and access to all drives and all folders	Not Defined
Registry		💹 Shutdown: Allow system to be shut down without having to log on	Not Defined
File System		🐻 Shutdown: Clear virtual memory pagefile	Not Defined
Wired Network (IEEE 802.3)	3) ≡	💹 System cryptography: Force strong key protection for user keys stored on the com	Not Defined
Windows Firewall with Adv	v	System cryptography: Use FIPS compliant algorithms for encryption, hashing, and	Enabled
📔 Network List Manager Poli	ic	🕎 System objectsi Require case insensitivity for non-Windows subsystems	Enabled

18. Unless a documented need exists, ensure Remote Desktop Sharing through NetMeeting is disabled.

Location Computer Configuration\Administrative Templates\Windows Components\NetMeeting\Disable Whiteboard

State		indows Components	4 🧾 Wi
 Enabled	le remote Desktop Sharing	ActiveX Installer Service	
		Add features to Windows 8	
		App Package Deployment	
		App runtime	2.70
		Application Compatibility	
		AutoPlay Policies	
		Biometrics	
		BitLocker Drive Encryption	Þ 🧰
		Credential User Interface	
		Desktop Gadgets	
		Desktop Window Manager	🖾 م
		Device and Driver Compati	2.7
		Digital Locker	15
		Edge UI	1
		Event Forwarding	
		Event Log Service 📃	Þ 🛄
		Event Viewer	
		Family Safety	
		File Explorer	Þ 🛄
		File History	2.5
		Game Explorer	
		HomeGroup	1
		Internet Explorer	🖾 م
		Internet Information Servic	27
		Location and Sensors	Þ 🧾
		Maintenance Scheduler	
		NetMeeting	1
		Digital Locker Edge UI Event Forwarding Event Log Service Event Viewer Family Safety File Explorer File History Game Explorer HomeGroup Internet Explorer Internet Explorer Internet Information Servic Location and Sensors Maintenance Scheduler NetMeeting	

19. Ensure the system is configured to disallow more than 1 remote terminal services connection, unless a documented need exists.

Allow 2 connections in Limit number of connects

Location Computer Configuration\Administrative Templates\Windows Components\Remote Desktop Services>Remote Desktop Sessions

Internet Information Servic	Setting	State	
Location and Sensors	E Allow remote start of unlisted programs	Not configured	
Maintenance Scheduler	Allow users to connect remotely by using Remote Desktop Services	Not configured	
NetMeeting	Automatic reconnection	Not configured	
Network Access Protection	Configure keep-alive connection interval	Not configured	
Network Projector	Deny logoff of an administrator logged in to the console session	Not configured	
OneDrive	Limit number of connections	Enabled	
Online Assistance	Restrict Remote Desktop Services users to a single Remote Desktop Servic	Not configured	
Password Synchronization	Select network detection on the server	Not configured	
Portable Operating System	E Select RDP transport protocols	Not configured	
Presentation Settings	Set rules for remote control of Remote Desktop Services user sessions	Not configured	
A BD Lissesing	Suspend user sign-in to complete app registration	Not configured	
RD Licensing	Turn off Fair Share CPU Scheduling	Not configured	
Remote Desktop Conne	The company of the contract of	-	
A P Remote Deskton Servio			
Application Compa			
Connections			
Device and Resourc =			
Licensing			
Printer Redirection			
Profiles			
RD Connection Brok			
Remote Session Env			
Security			
Session Time Limits			
Temporary folders			

20. Ensure the system is configured to use terminal services temporary folders on a "per session" basis, and that the temporary folders are deleted when a terminal services session is terminated.

Use default. No change.

21. The time limit for idle, and disconnected terminal services sessions should comply with organizational or regulatory standards.

Use default. No change.

22. Configure the system to disallow the installation of kernel-mode printer drivers. Then navigate to the following path and locate "Disallow installation of printers using kernel-mode drivers" and set to disable.

Local computer Policy---->Computer Configuration---->Administrative Templates---->Printers---->"Disallow installation of printers using kernel-mode drivers" to set enable.



23. Ensure the system is configured to use SafeDLLSearchMode.

Configure the policy value for Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Security Options -> "MSS: (SafeDIISearchMode) Enable Safe DLL search mode (recommended)" to "Enabled".

If the value for "MSS: (SafeDIISearchMode) Enable Safe DLL search mode (recommended)" is not set to "Enabled", then this is a finding.

The policy referenced configures the following registry value:

Registry Hive: HKEY_LOCAL_MACHINE Registry Path: \System\CurrentControlSet\Control\Session Manager\

Value Name: SafeDllSearchMode

Value Type: REG_DWORD Value: 1

Ø		Registry Editor		_ 0 ×
File Edit View I	avorites Help			
Þ	- Power 🗠	Name	Туре	Data
Þ	- 👪 Print	ab (Default)	REG_SZ	(value not set)
	PriorityControl	100 AutoChkTimeout	REG_DWORD	0x0000000a (10)
	ProductOptions	ab BootExecute	REG_MULTI_SZ	autocheck autochk /q /v *
Þ	JafeBoot	ab BootShell	REG_EXPAND_SZ	%SystemRoot%\system32\bootin
	ScEvents	38 CriticalSectionTimeout	REG_DWORD	0x00278d00 (2592000)
Þ	ScsiPort	ab ExcludeFromKnownDlls	REG_MULTI_SZ	
	SecureBoot	🕫 GlobalFlag	REG_DWORD	0x00000000 (0)
Þ	SecurePipeServers	HeapDeCommitFreeBloc	REG_DWORD	0x00000000 (0)
Þ	SecurityProviders	HeapDeCommitTotalFree	REG DWORD	0x00000000 (0)
	Server Applications	100 HeapSegmentCommit	REG DWORD	0x00000000 (0)
	ServiceGroupOrder	116 HeapSegmentReserve	REG DWORD	0x00000000 (0)
	ServiceProvider	100 NumberOfInitialSessions	REG DWORD	0x00000002 (2)
	SOMServicel int	ab ObjectDirectories	REG MULTI SZ	\Windows \RPC Control
N N	Srn =	ab PendingFileRenameOper	REG MULTI SZ	\??\C:\Windows\system32\spool
	SrpExtensionConfig	100 ProcessorControl	REG DWORD	0x00000002 (2)
b	J Stillmage	ProtectionMode	REG DWORD	0x00000001 (1)
Þ	Storage	ResourceTimeoutCount	REG DWORD	0x0009e340 (648000)
Þ	Je StorageManagement	ab RunLevelExecute	REG MULTI SZ	WinInit ServiceControlManager
	Je StorPort	ab RunLevelValidate	REG MULTI SZ	ServiceControlManager
	SystemInformation	ab SETUPEXECUTE	REG MULTI SZ	
Þ	SystemResources	SafeDIISearchMode	REG_DWORD	0x00000001 (1)

24. The system should be configured to disallow "Windows Media Player from conducting automatic updates, and automatic CODEC downloads".

Enable Windows Media Player to periodically check for updates by using a Group Policy setting

To enable Windows Media Player to automatically check for updates by using a Group Policy setting, follow these steps:

- In Group Policy Microsoft Management Console (MMC), under Computer Configuration expand Administrative Templates, expand Windows Components, and then click Windows Media Player.
- 2. In the list of available policies, double-click **Prevent Automatic Updates**.
- 3. Click **Disabled** or click **Not Configured**, and then click **OK**.
- 4. Close Group Policy MMC.



25. For Domain Controllers, ensure the system is configured to sign all LDAP data sent to clients. Domain controller: LDAP server signing requirements to Require signature Location²

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

- Removed from Default Domain Controller Policy (from the second seco	Policy	Policy Setting
🖌 👰 Computer Configuration	Ship Scustom SD%	Not Defined
a 🚞 Policies	S %DSCustomSD%	Not Defined
Software Settings	SFRSCustomSD%	Not Defined
⊿	Accounts: Administrator account status	Not Defined
Name Resolution Policy	Accounts: Block Microsoft accounts	Not Defined
Scripts (Startup/Shutdown)	Accounts: Guest account status	Not Defined
Deployed Printers	Accounts: Limit local account use of blank passwords to console logon only	Not Defined
Security Settings	Accounts: Rename administrator account	Not Defined
Account Policies	Accounts: Rename quest account	Not Defined
a 📓 Local Policies	Audit: Audit the access of global system objects	Not Defined
Audit Policy	Audit: Audit the use of Backup and Restore privilege	Not Defined
User Rights Assignment	Audit: Force audit policy subcategory settings (Windows Vista or later) to override	Not Defined
Security Options	Audit: Shut down system immediately if unable to lon security audits	Not Defined
Participad Groups	DCOM: Machine Access Restrictions in Security Descriptor Definition Language (S.	Not Defined
Custeen Services	DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (S	Not Defined
System Services	Device: Allow undock without having to log on	Not Defined
Ele Surtem	Device: Allowed to format and elect removable media	Not Defined
Wind Natural (IEEE 802 3) Polician	Devices Prevent warr from installing printer driver	Not Defined
Windows Firewall with Advanced Securit	Devices: Prevent users from installing printer drivers	Not Defined
Natural List Manager Policies	Devices: Restrict CD-ROM access to locally logged-on user only	Not Defined
Wireless Network (ISE 802 11) Delicies	Devices: Restrict floppy access to locally logged-on user only	Not Defined
Dublic Key Policies	Domain controller: Allow server operators to schedule tasks	Not Defined
 Coftware Restriction Dolicies 	Domain controller: LDAP server signing requirements	Require signing

26. Configure the system to software certificate restriction rules.

Enable System settings: Use certificate rules on Windows executables for Software Restriction Policies Location[®]

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



27. Configure the system to match domain-based registry policies No change.

28. The system should be configured to disallow DCOM object calls from all users except Administrators. Use the default settings. No change.

29. Ensure the system is configured to disallow the ability to "turn off background refresh of Group Policy."

Location: Computer Configuration\Administrative Templates\System\Group Policy



30. Ensure that User Account Control has not been disabled. Use the default. No change.

Configure the system to require Admin Approval mode for User Account Control for the built-in Administrator account, and that the Administrator is prompted for credentials.

31. Configure the system to require Admin Approval mode for User Account Control for the built-in Administrator account, and that the Administrator is prompted for credentials.

User Account Control: Admin Approval Mode for the Built-in Administrator account

Location **?**

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

		· · · · · · · · · · · · · · · · · · ·
- Removed from Default Domain Controller Policy (fr ^	Policy	Policy Setting
a 🙀 Computer Configuration	Network security: LDAP client signing requirements	Not Defined
a 🧾 Policies	Retwork security: Minimum session security for NTLM SSP based (including secur	Not Defined
Software Settings	Network security: Minimum session security for NTLM SSP based (including secur	Not Defined
Windows Settings	Network security: Restrict NTLM: Add remote server exceptions for NTLM authenti	Not Defined
Name Resolution Policy	Network security: Restrict NTLM: Add server exceptions in this domain	Not Defined
Scripts (Startup/Shutdown)	Network security: Restrict NTLM: Audit Incoming NTLM Traffic	Not Defined
Deployed Printers	Network security: Restrict NTLM: Audit NTLM authentication in this domain	Not Defined
A Basecurity Settings	Network security: Restrict NTLM: Incoming NTLM traffic	Not Defined
Account Policies	Network security: Restrict NTLM: NTLM authentication in this domain	Not Defined
A Local Policies	Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers	Not Defined
Addit Policy	Recovery console: Allow automatic administrative logon	Not Defined
Security Ontions	Recovery console: Allow floppy copy and access to all drives and all folders	Not Defined
Event Log	Shutdown: Allow system to be shut down without having to log on	Not Defined
Restricted Groups	Shutdown: Clear virtual memory pagefile	Not Defined
System Services	System cryptography: Force strong key protection for user keys stored on the com	Not Defined
Registry	System cryptography: Use FIPS compliant algorithms for encryption, hashing, and	Enabled
File System	System objects: Require case insensitivity for non-Windows subsystems	Enabled
Wired Network (IEEE 802.3) Policies	System objects: Strengthen default permissions of internal system objects (e.g. Sy	Not Defined
Windows Firewall with Advanced Securit	System settings: Optional subsystems	Not Defined
Network List Manager Policies	System settings: Use Certificate Rules on Windows Executables for Software Restric	Enabled
Wireless Network (IEEE 802.11) Policies	User Account Control: Admin Approval Mode for the Built-in Administrator account	Enabled
		and the second

32. The system should have User Account Control configured to automatically deny elevation requests from regular users.

User Account Control: Behavior of the elevation prompt for standard users

Location?

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



33. User Account Control should be configured to prompt for elevation for any application installations, and only applications which are installed in secure locations to run with elevated privileges. User Account Control: Detect application installations and prompt for elevation

Location?

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



34. Ensure the system is configured to require "secure desktop mode" when prompting for UAC elevation.

User Account Control: Switch to the secure desktop when prompting for elevation

Location **?**

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

Removed from Default Domain Controller Policy (fr	Policy	Policy Setting
4 👰 Computer Configuration	Network security: LDAP client signing requirements	Not Defined
a 🚞 Policies	Network security: Minimum session security for NTLM SSP based (including secur	Not Defined
Software Settings	Network security: Minimum session security for NTLM SSP based (including secur	Not Defined
a 🛄 Windows Settings	Network security: Restrict NTLM: Add remote server exceptions for NTLM authenti	Not Defined
D Mame Resolution Policy	Network security: Restrict NTLM: Add server exceptions in this domain	Not Defined
Scripts (Startup/Shutdown)	Network security: Restrict NTLM: Audit Incoming NTLM Traffic	Not Defined
Deployed Printers	Network security: Restrict NTLM: Audit NTLM authentication in this domain	Not Defined
A has Security Settings	Network security: Restrict NTLM: Incoming NTLM traffic	Not Defined
Account Policies	Network security: Restrict NTLM: NTLM authentication in this domain	Not Defined
A J Local Policies	Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers	Not Defined
Audit Policy	Recovery console: Allow automatic administrative logon	Not Defined
Security Options	Recovery console: Allow floppy copy and access to all drives and all folders	Not Defined
Event log	Shutdown: Allow system to be shut down without having to log on	Not Defined
h Restricted Groups	Shutdown: Clear virtual memory pagefile	Not Defined
System Services	System cryptography: Force strong key protection for user keys stored on the com	Not Defined
b Control Registry	System cryptography: Use FIPS compliant algorithms for encryption, hashing, and	Enabled
File System	System objects: Require case insensitivity for non-Windows subsystems	Enabled
Wired Network (IEEE 802.3) Policies	System objects: Strengthen default permissions of internal system objects (e.g. Sy	Not Defined
Windows Firewall with Advanced Securit	System settings: Optional subsystems	Not Defined
Network List Manager Policies	System settings: Use Certificate Rules on Windows Executables for Software Restric	Enabled
Wireless Network (IEEE 802.11) Policies	SUser Account Control: Admin Approval Mode for the Built-in Administrator account	Enabled
Public Key Policies	User Account Control: Allow UlAccess applications to prompt for elevation withou	Not Defined
Software Restriction Policies	B User Account Control: Behavior of the elevation prompt for administrators in Admi	Prompt for credentials
Network Access Protection	SUser Account Control: Behavior of the elevation prompt for standard users	Prompt for credentials
Application Control Policies	User Account Control: Detect application installations and prompt for elevation	Not Defined
IP Security Policies on Active Directory (User Account Control: Only elevate executables that are signed and validated	Not Defined
Advanced Audit Policy Configuration	R User Account Control: Only elevate UIAccess applications that are installed in secur	Not Defined
Administrative Templates Policy definitions (A	Q User Account Control: Run all administrators in Admin Approval Mode	Not Defined
b Control Panel	Super Account Control: Switch to the secure desktop when prompting for elevation	Enabled

35. Configure the system to run non-UAC compliant applications in a virtualized state.

User Account Control: Run all administrators in Admin Approval Mode No change.

36. The system should be configured to disallow the enumeration of administrator accounts upon elevation.

Navigate to "Local Computer Policy", "Computer Configuration" "Administrative Templates", "Windows Components", "Credential User Interface".

Set "Enumerate administrator accounts on elevation" to "disabled".

BitLocker Drive Encryption	Setting	State
🚞 Credential User Interface	Do not display the password reveal button	Not configured
Desktop Gadgets	Enumerate administrator accounts on elevation	Disabled
Desktop Window Manager Device and Driver Compatibility	E Require trusted path for credential entry	Not configured

37. Ensure that the system is set to disallow the redirection of shared drives during terminal services sessions.

Procedure

In the Group Policy Editor, go to Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Device and Resource Redirection. Enable the Do not allow drive redirection group policy setting

Maintenance Scheduler	Setting A	State
NetMeeting	E Allow audio and video playback redirection	Not configured
Network Access Protection	E Allow audio recording redirection	Not configured
Network Projector	Allow time zone redirection	Not configured
ConeDrive OneDrive	Do not allow Clipboard redirection	Not configured
Online Assistance	Do not allow COM port redirection	Not configured
Password Synchronization	Do not allow drive redirection	Enabled
Portable Operating System	E Do not allow LPT port redirection	Not configured
Presentation Settings	Do not allow smart card device redirection	Not configured
A Remote Desktop Services	The not allow supported Plug and Play device redirection	Not configured
RD Licensing Remote Desktop Connection Client	E Limit audio playback quality	Not configured
a 🚞 Remote Desktop Session Host		
Application Compatibility		
Connections	1	
Device and Resource Redirection		

38. Configure the system to disallow the ability to publish to the web via the files and folders task scheduler.

I familie a

Navigate to the following section: Computer Configuration > Administrative Templates > System > Internet Communication Management > Internet Communication settings.

Disk Quotas	Setting	State
Distributed COM	Turn off access to all Windows Update features	Not configured
Criver Installation	I Turn off access to the Store	Not configured
Early Launch Antimalware	Turn off Automatic Root Certificates Update	Not configured
File Classification Infrastructure	Turn off downloading of print drivers over HTTP	Not configured
File Share Shadow Copy Provider	Turn off Event Viewer "Events.asp" links	Not configured
Filesystem	E Turn off handwriting recognition error reporting	Not configured
Folder Redirection	Turn off Help and Support Center "Did you know?" content	Not configured
Group Policy	Turn off Help and Support Center Microsoft Knowledge Base search	Not configured
Internet Communication Management	Turn off Internet Connection Wizard if URL connection is referring to Microsoft.com	Not configured
N C iscsi	Turn off Internet download for Web publishing and online ordering wizards	Enabled
KDC	Turn off Internet File Association service	Not configured
Kerberos	Turn off printing over HTTP	Not configured
Locale Services	Turn off Registration if URL connection is referring to Microsoft.com	Not configured
Cogon Logon	E Turn off Search Companion content file updates	Not configured
Net Logon	E Turn off the "Order Prints" picture task	Not configured
Power Management	Turn off the "Publish to Web" task for files and folders	Enabled

39. The system should be configured to disallow downloading provider lists for Web publishing, and online ordering wizards.

Navigate to the following section: Computer Configuration > Administrative Templates > System > Internet Communication Management > Internet Communication settings.

📄 Disk Quotas 🗸	Setting	State
Distributed COM	Turn off access to all Windows Update features	Not configured
Driver Installation	E Turn off access to the Store	Not configured
Early Launch Antimalware	15 Turn off Automatic Root Certificates Update	Not configured
File Classification Infrastructure	E Turn off downloading of print drivers over HTTP	Not configured
File Share Shadow Copy Provider	🔚 Turn off Event Viewer "Events.asp" links	Not configured
▷ III Filesystem	E Turn off handwriting recognition error reporting	Not configured
Folder Redirection	E Turn off Help and Support Center "Did you know?" content	Not configured
Group Policy	E Turn off Help and Support Center Microsoft Knowledge Base search	Not configured
Internet Communication Management	E Turn off Internet Connection Wizard if URL connection is referring to Microsoft.com	Not configured
Internet Communication settings	Turn off Internet download for Web publishing and online ordering wizards	Enabled
v incer		

40. The system should be configured to prevent Windows Messenger Customer Experience Improvement program data collection.

Navigate to the following section: Computer Configuration > Administrative Templates > System > Internet Communication Management > Internet Communication settings.

🛗 Disk Quotas 🗸	Setting	State
Distributed COM	Turn off access to all Windows Update features	Not configured
Driver Installation	Turn off access to the Store	Not configured
Early Launch Antimalware	E Turn off Automatic Root Certificates Update	Not configured
File Classification Infrastructure	Turn off downloading of print drivers over HTTP	Not configured
File Share Shadow Copy Provider	Turn off Event Viewer "Events.asp" links	Not configured
Filesystem	E Turn off handwriting recognition error reporting	Not configured
Folder Redirection	Turn off Help and Support Center "Did you know?" content	Not configured
Group Policy	Turn off Help and Support Center Microsoft Knowledge Base search	Not configured
Internet Communication Management	Turn off Internet Connection Wizard if URL connection is referring to Microsoft.com	Not configured
Internet Communication settings	Turn off Internet download for Web publishing and online ordering wizards	Enabled
	Turn off Internet File Association service	Not configured
Kerberos	Turn off printing over HTTP	Not configured
Locale Services	Turn off Registration if URL connection is referring to Microsoft.com	Not configured
Logon	E Turn off Search Companion content file updates	Not configured
> 📑 Net Logon	Turn off the "Order Prints" picture task	Not configured
Power Management	Turn off the "Publish to Web" task for files and folders	Enabled
📔 Recovery	Turn off the Windows Messenger Customer Experience Improvement Program	Enabled

41. Ensure the system is not allowing the downloading of program and file content updates via Search Companion.

Configure the policy value for Computer Configuration -> Administrative Templates -> System -> Internet Communication Management -> Internet Communication setting 'Turn off Search Companion content file updates' to "Enabled".

🛅 Disk Quotas	~	Setting	State
Distributed COM Driver Installation Early Launch Antimalware File Classification Infrastructure File Share Shadow Copy Provider		Turn off access to all Windows Update features	Not configured
		Turn off access to the Store	Not configured
		Turn off Automatic Root Certificates Update	Not configured
		Turn off downloading of print drivers over HTTP	Not configured
		Turn off Event Viewer "Events.asp" links	Not configured
▷ III Filesystem		Turn off handwriting recognition error reporting	Not configured
Folder Redirection		Turn off Help and Support Center "Did you know?" content	Not configured
Group Policy			Not configured
Internet Communication Management		Turn off Internet Connection Wizard if URL connection is referring to Microsoft.com	Not configured
internet Communication settings		E Turn off Internet download for Web publishing and online ordering wizards	Enabled
KDC		E Turn off Internet File Association service	Not configured
Kerberos		E Turn off printing over HTTP	Not configured
Locale Services		E Turn off Registration if URL connection is referring to Microsoft.com	Not configured
		Turn off Search Companion content file updates	Enabled

42. Configure the system to disable the ability to download drivers via Windows Update. No change.

43. Ensure "system shell protected mode" is enabled. No change

44. The system should be configured to disallow the ability for "UIAccess applications to prompt for elevation without using the secure desktop."

User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop

Location Computer Configuration/Windows Settings/Security Settings/Local Policies/Security Options

Removed from Default Domain Controller Policy (feedback)	Policy	Policy Setting
🖌 👰 Computer Configuration	Network security: Force logoff when logon hours expire	Not Defined
a 🛄 Policies	C Network security: LAN Manager authentication level	Send NTLM response only
b Software Settings	Retwork security: LDAP client signing requirements	Not Defined
🖬 🔛 Windows Settings	Retwork security: Minimum session security for NTLM SSP based (including secur	Not Defined
Name Resolution Policy	Network security: Minimum session security for NTLM SSP based (including secur	Not Defined
Scripts (Startup/Shutdown)	Network security: Restrict NTLM: Add remote server exceptions for NTLM authenti	Not Defined
Deployed Printers	Network security: Restrict NTLM: Add server exceptions in this domain	Not Defined
A Security Settings	Network security: Restrict NTLM: Audit Incoming NTLM Traffic	Not Defined
Account Policies	Network security: Restrict NTLM: Audit NTLM authentication in this domain	Not Defined
A Local Policies	Network security: Restrict NTLM: Incoming NTLM traffic	Not Defined
Ilser Rights Assignment	Retwork security: Restrict NTLM: NTLM authentication in this domain	Not Defined
Security Options	Retwork security: Restrict NTLM: Outgoing NTLM traffic to remote servers	Not Defined
b Event Log	Recovery console: Allow automatic administrative logon	Not Defined
Restricted Groups	Recovery console: Allow floppy copy and access to all drives and all folders	Not Defined
System Services	Shutdown: Allow system to be shut down without having to log on	Not Defined
Registry	E Shutdown: Clear virtual memory pagefile	Not Defined
File System	System cryptography: Force strong key protection for user keys stored on the com	Not Defined
Wired Network (IEEE 802.3) Policies	System cryptography: Use FIPS compliant algorithms for encryption, hashing, and	Enabled
Windows Firewall with Advanced Securit	System objects: Require case insensitivity for non-Windows subsystems	Enabled
Network List Manager Policies	System objects: Strengthen default permissions of internal system objects (e.g. Sy	Not Defined
Wireless Network (IEEE 802.11) Policies	System settings: Optional subsystems	Not Defined
Public Key Policies	System settings: Use Certificate Rules on Windows Executables for Software Restric	Enabled
Software Restriction Policies	User Account Control: Admin Approval Mode for the Built-in Administrator account	Enabled
Network Access Protection	User Account Control: Allow UlAccess applications to prompt for elevation withou	Disabled

45. Ensure that all unnecessary features in the "Server Manager" are disabled.