Device-BSI-SiSyPHuS-normal-V1.1

Data collected on: 27.03.2025 13:33:12

General

hide

Details

hide

Domain	[redacted]
Owner	[redacted]
Created	23.10.2024 15:49:36
Modified	27.03.2025 12:42:16
User Revisions	1 (AD), 1 (SYSVOL)
Computer Revisions	376 (AD), 376 (SYSVOL)
Unique ID	{6DDF78C2-AAE1-4E5C-A2B1-06D31349D9B0}
GPO Status	Enabled

Links

hide

Location	Enforced	Link Status	Path
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

This list only includes links in the domain of the GPO.

Security Filtering

hide

The settings in this GPO can only apply to the following groups, users, and computers:

Name
[redacted]

Delegation

hide

These groups and users have the specified permission for this GPO

Name	Allowed Permissions	Inherited
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Computer Configuration (Enabled)

hide

Policies

hide

Windows Settings

hide

Security Settings hide

Account Policies/Password Policy hide

Policy	Setting
Enforce password history	24 passwords remembered
Minimum password length	14 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

Local Policies/Security Options hide

Accounts hide

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

Audit hide

Policy	Setting
Audit: Audit the access of global system objects	Disabled

Devices hide

Policy	Setting
Devices: Allowed to format and eject removable media	Administrators and Interactive Users

Domain Member hide

Policy	Setting
Domain member: Digitally encrypt or sign secure channel data (always)	Enabled
Domain member: Digitally encrypt secure channel data (when possible)	Enabled
Domain member: Digitally sign secure channel data (when possible)	Enabled
Domain member: Disable machine account password changes	Disabled
Domain member: Maximum machine account password age	30 days
Domain member: Require strong (Windows 2000 or later) session key	Enabled

Interactive Logon hide

Policy	Setting
Interactive logon: Do not require CTRL+ALT+DEL	Disabled
Interactive logon: Prompt user to change password before expiration	14 days
Interactive logon: Smart card removal behavior	Lock Workstation

Microsoft Network Client hide

Policy	Setting
Microsoft network client: Digitally sign communications (always)	Enabled

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

Microsoft Network Server hide

Policy	Setting
Microsoft network server: Amount of idle time required before suspending session	15 minutes
Microsoft network server: Digitally sign communications (always)	Enabled
Microsoft network server: Digitally sign communications (if client agrees)	Enabled
Microsoft network server: Disconnect clients when logon hours expire	Enabled

Network Access hide

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

Network Security hide

Policy	Setting
Network security: Do not store LAN Manager hash value on next password change	Enabled
Network security: Force logoff when logon hours expire	Enabled

Network security: LAN Manager authentication level	Send NTLMv2 response only
Network security: LDAP client signing requirements	Negotiate signing
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients	Enabled
Require NTLMv2 session security	Enabled
Require 128-bit encryption	Enabled
Network security: Minimum session security for NTLM SSP based (including secure RPC) servers	Enabled
Require NTLMv2 session security	Enabled
Require 128-bit encryption	Enabled

System Objects

hide

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

User Account Control

hide

Policy	Setting
User Account Control: Admin Approval Mode for the Built-in Administrator account	Enabled
User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop	Disabled
User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode	Prompt for consent on the secure desktop
User Account Control: Behavior of the elevation prompt for standard users	Prompt for credentials on the secure desktop
User Account Control: Detect application installations and prompt for elevation	Enabled
User Account Control: Only elevate UIAccess applications that are installed in secure locations	Enabled
User Account Control: Run all administrators in Admin Approval Mode	Enabled
User Account Control: Switch to the secure desktop when prompting for elevation	Enabled
User Account Control: Virtualize file and registry write failures to per-user locations	Enabled

Other

hide

Policy	Setting
Accounts: Block Microsoft accounts	Users can't add or log on with Microsoft accounts
Interactive logon: Machine account lockout threshold	10 invalid logon attempts
Interactive logon: Machine inactivity limit	900 seconds
Microsoft network server: Server SPN target name validation level	Accept if provided by client
Network access: Restrict clients allowed to make remote calls to SAM	"O:BAG:BAD:(A;;RC;;;BA)(A;;RC;;;AU)"

Network security: Allow Local System to use computer identity for NTLM	Enabled
Network security: Allow LocalSystem NULL session fallback	Disabled
Network security: Allow PKU2U authentication requests to this computer to use online identities.	Disabled
Network security: Configure encryption types allowed for Kerberos	Enabled

DES_CBC_CRC	Disabled
DES_CBC_MD5	Disabled
RC4_HMAC_MD5	Enabled
AES128_HMAC_SHA1	Enabled
AES256_HMAC_SHA1	Enabled
Future encryption types	Enabled

System Services hide

Browser (Startup Mode: Disabled) hide

Permissions
No permissions specified

Auditing
No auditing specified

Connected User Experiences and Telemetry (Startup Mode: Disabled) hide

Permissions
No permissions specified

Auditing
No auditing specified

icssvc (Startup Mode: Disabled) hide

Permissions
No permissions specified

Auditing
No auditing specified

irmon (Startup Mode: Disabled) hide

Permissions
No permissions specified

Auditing
No auditing specified

Routing and Remote Access (Startup Mode: Disabled) hide

Permissions
No permissions specified

Auditing
No auditing specified

Remote Procedure Call (RPC) Locator (Startup Mode: Disabled) hide

Permissions
No permissions specified

Auditing
No auditing specified

Internet Connection Sharing (ICS) (Startup Mode: Disabled) hide

Permissions
No permissions specified

Auditing
No auditing specified

SSDP Discovery (Startup Mode: Disabled) hide

Permissions
No permissions specified

Auditing
No auditing specified

UPnP Device Host (Startup Mode: Disabled) hide

Permissions
No permissions specified

Auditing
No auditing specified

Windows Media Player Network Sharing Service (Startup Mode: Disabled) hide

Permissions
No permissions specified

Auditing
No auditing specified

XblAuthManager (Startup Mode: Disabled) hide

Permissions
No permissions specified

Auditing
No auditing specified

XblGameSave (Startup Mode: Disabled) hide

Permissions
No permissions specified

Auditing
No auditing specified

XboxGipSvc (Startup Mode: Disabled) hide

Permissions
No permissions specified

Auditing
No auditing specified

XboxNetApiSvc (Startup Mode: Disabled) hide

Permissions
No permissions specified

Auditing
No auditing specified

Windows Firewall with Advanced Security hide

Global Settings hide

Policy	Setting
Policy version	2.29
Disable stateful FTP	Not Configured
Disable stateful PPTP	Not Configured
IPsec exempt	Not Configured
IPsec through NAT	Not Configured
Preshared key encoding	Not Configured
SA idle time	Not Configured
Strong CRL check	Not Configured

Domain Profile Settings hide

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

Private Profile Settings hide

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

Public Profile Settings hide

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

Connection Security Settings hide

Administrative Templates hide

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

Control Panel/Personalization

Policy	Setting	Comment
Prevent enabling lock screen camera	Enabled	
Prevent enabling lock screen slide show	Enabled	

Control Panel/Regional and Language Options hide

Policy	Setting	Comment
Allow users to enable online speech recognition services	Disabled	

Control Panel/Regional and Language Options/Handwriting personalization hide

Policy	Setting	Comment
Turn off automatic learning	Enabled	

MS Security Guide hide

Policy	Setting	Comment
Apply UAC restrictions to local accounts on network logons	Enabled	
Configure SMB v1 client driver	Enabled	
Configure MrxSmb10 driver	Disable driver (recommended)	

Policy	Setting	Comment
Configure SMB v1 server	Disabled	
Enable Structured Exception Handling Overwrite Protection (SEHOP)	Enabled	
LSA Protection	Enabled	
NetBT NodeType configuration	Enabled	
Configure NetBT NodeType	P-node (recommended)	

Policy	Setting	Comment
WDigest Authentication (disabling may require KB2871997)	Disabled	

MSS (Legacy) hide

Policy	Setting	Comment
MSS: (AutoAdminLogon) Enable Automatic Logon	Disabled	
MSS: (DisableIPSourceRouting IPv6) IP source routing protection level	Enabled	
DisableIPSourceRoutingIPv6	Highest protection, source routing is completely disabled	

Policy	Setting	Comment
MSS: (DisableIPSourceRouting) IP source routing protection level	Enabled	
DisableIPSourceRouting	Highest protection, source routing is completely disabled	

Policy	Setting	Comment

MSS: (EnableDeadGWDetect) Allow automatic detection of dead network gateways	Disabled
MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes	Disabled
MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers	Enabled
MSS: (SafeDllSearchMode) Enable Safe DLL search mode	Enabled
MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires	Enabled

ScreenSaverGracePeriod	5

Network/DNS Client hide

Policy	Setting	Comment
Turn off multicast name resolution	Enabled	

Network/Lanman Workstation hide

Policy	Setting	Comment
Enable insecure guest logons	Disabled	

Network/Network Connections hide

Policy	Setting	Comment
Prohibit installation and configuration of Network Bridge on your DNS domain network	Enabled	
Prohibit use of Internet Connection Sharing on your DNS domain network	Enabled	
Require domain users to elevate when setting a network's location	Enabled	

Network/Network Connections/Windows Defender Firewall/Domain Profile hide

Policy	Setting	Comment
Windows Defender Firewall: Prohibit notifications	Enabled	
Windows Defender Firewall: Protect all network connections	Enabled	

Network/Network Provider hide

Policy	Setting	Comment
Hardened UNC Paths	Enabled	

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

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

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

Network/Windows Connection Manager hide

Policy	Setting	Comment
Minimize the number of simultaneous connections to the Internet or a Windows Domain	Enabled	

Minimize Policy Options	1 = Minimize simultaneous connections

Policy	Setting	Comment
Prohibit connection to non-domain networks when connected to domain authenticated network	Enabled	

Network/WLAN Service/WLAN Settings hide

Policy	Setting	Comment
Allow Windows to automatically connect to suggested open hotspots, to networks shared by contacts, and to hotspots offering paid services	Disabled	

System/Credentials Delegation hide

Policy	Setting	Comment
Encryption Oracle Remediation	Enabled	

Protection Level:	Force Updated Clients

Policy	Setting	Comment
Remote host allows delegation of non-exportable credentials	Enabled	

System/Device Installation/Device Installation Restrictions hide

Policy	Setting	Comment
Prevent installation of devices using drivers that match these device setup classes	Enabled	

Prevent installation of devices using drivers for these device setup classes:
{7ebefbc0-3200-11d2-b4c2-00a0C9697d07}
{c06ff265-ae09-48f0-812c-16753d7cba83}
{6bdd1fc1-810f-11d0-bec7-08002be2092f}

To create a list of device classes, click Show. In the Show Contents dialog box, in the Value column, type a GUID that represents a device setup class

(for example, {25DBCE51-6C8F-4A72-8A6D-B54C2B4FC835}).	
Also apply to matching devices that are already installed.	Enabled

System/Early Launch Antimalware hide

Policy	Setting	Comment
Boot-Start Driver Initialization Policy	Enabled	
Choose the boot-start drivers that can be initialized:	Good, unknown and bad but critical	

System/Group Policy hide

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

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

Policy	Setting	Comment
Continue experiences on this device	Disabled	
Turn off background refresh of Group Policy	Disabled	

System/Internet Communication Management/Internet Communication settings hide

Policy	Setting	Comment
Turn off downloading of print drivers over HTTP	Enabled	
Turn off Internet download for Web publishing and online ordering wizards	Enabled	

System/Kernel DMA Protection hide

Policy	Setting	Comment
Enumeration policy for external devices incompatible with Kernel DMA Protection	Enabled	
Enumeration policy	Block all	

System/Logon hide

Policy	Setting	Comment
Block user from showing account details on sign-in	Enabled	
Do not display network selection UI	Enabled	
Do not enumerate connected users on domain-joined computers	Enabled	
Enumerate local users on domain-joined computers	Disabled	

Turn off app notifications on the lock screen	Enabled
Turn off picture password sign-in	Enabled
Turn on convenience PIN sign-in	Disabled

System/Power Management/Sleep Settings hide

Policy	Setting	Comment
Allow network connectivity during connected-standby (on battery)	Disabled	
Allow network connectivity during connected-standby (plugged in)	Disabled	
Allow standby states (S1-S3) when sleeping (on battery)	Disabled	
Allow standby states (S1-S3) when sleeping (plugged in)	Disabled	
Require a password when a computer wakes (on battery)	Enabled	
Require a password when a computer wakes (plugged in)	Enabled	

System/Remote Assistance hide

Policy	Setting	Comment
Configure Offer Remote Assistance	Disabled	
Configure Solicited Remote Assistance	Disabled	

System/Remote Procedure Call hide

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

System/Trusted Platform Module Services hide

Policy	Setting	Comment
Ignore the default list of blocked TPM commands	Disabled	
Standard User Lockout Duration	Enabled	
Duration for counting TPM authorization failures (minutes):	30	

Policy	Setting	Comment
Standard User Total Lockout Threshold	Enabled	
Maximum number of authorization failures per duration:	5	

Windows Components/App runtime hide

Policy	Setting	Comment
Allow Microsoft accounts to be optional	Enabled	

Windows Components/AutoPlay Policies hide

Policy	Setting	Comment
Disallow Autoplay for non-volume devices	Enabled	
Set the default behavior for AutoRun	Enabled	
Default AutoRun Behavior	Do not execute any autorun commands	

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

Windows Components/Biometrics/Facial Features hide

Policy	Setting	Comment
Configure enhanced anti-spoofing	Enabled	

Windows Components/Cloud Content hide

Policy	Setting	Comment
Turn off Microsoft consumer experiences	Enabled	

Windows Components/Connect hide

Policy	Setting	Comment
Require pin for pairing	Enabled	
Choose one of the following actions	Always	

Windows Components/Credential User Interface hide

Policy	Setting	Comment
Do not display the password reveal button	Enabled	
Enumerate administrator accounts on elevation	Disabled	

Windows Components/Data Collection and Preview Builds hide

Policy	Setting	Comment
Allow device name to be sent in Windows diagnostic data	Disabled	
Allow Diagnostic Data	Enabled	
	Diagnostic data off (not recommended)	

Policy	Setting	Comment
Do not show feedback notifications	Enabled	
Toggle user control over Insider builds	Disabled	

Windows Components/Delivery Optimization hide

Policy	Setting	Comment
Download Mode	Enabled	

Download Mode:	Simple (99)

Windows Components/File Explorer hide

Policy	Setting	Comment
Turn off Data Execution Prevention for Explorer	Disabled	
Turn off heap termination on corruption	Disabled	
Turn off shell protocol protected mode	Disabled	

Windows Components/Microsoft account hide

Policy	Setting	Comment
Block all consumer Microsoft account user authentication	Enabled	

Windows Components/Microsoft Defender Antivirus hide

Policy	Setting	Comment
Configure detection for potentially unwanted applications	Enabled	

Policy	Setting	Comment
Turn off Microsoft Defender Antivirus	Disabled	

Windows Components/Microsoft Defender Antivirus/MAPS hide

Policy	Setting	Comment
Configure local setting override for reporting to Microsoft MAPS	Disabled	

Windows Components/Microsoft Defender Antivirus/Microsoft Defender Exploit Guard/Attack Surface Reduction hide

Policy	Setting	Comment
Configure Attack Surface Reduction rules	Enabled	

Set the state for each ASR rule:	
26190899-1602-49e8-8b27-eb1d0a1ce869	1
3b576869-a4ec-4529-8536-b80a7769e899	1
5beb7efe-fd9a-4556-801d-275e5ffc04cc	1
75668c1f-73b5-4cf0-bb93-3ecf5cb7cc84	1
7674ba52-37eb-4a4f-a9a1-f0f9a1619a2c	1
92e97fa1-2edf-4476-bdd6-9dd0b4dddc7b	1
9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2	1
b2b3f03d-6a65-4f7b-a9c7-1c7ef74a9ba4	1
be9ba2d9-53ea-4cdc-84e5-9b1eeee46550	1
d3e037e1-3eb8-44c8-a917-57927947596d	1
d4f940ab-401b-4efc-aadc-ad5f3c50688a	1

Windows Components/Microsoft Defender Antivirus/Microsoft Defender Exploit Guard/Network Protection hide

Policy	Setting	Comment
Prevent users and apps from accessing dangerous websites	Enabled	

Windows Components/Microsoft Defender Antivirus/Real-time Protection hide

Policy	Setting	Comment
Turn on behavior monitoring	Enabled	

Windows Components/Microsoft Defender Antivirus/Reporting hide

Policy	Setting	Comment
Configure Watson events	Disabled	

Windows Components/Microsoft Defender Antivirus/Scan hide

Policy	Setting	Comment
Scan removable drives	Enabled	
Turn on e-mail scanning	Enabled	

Windows Components/Microsoft Edge hide

Policy	Setting	Comment
Configure Windows Defender SmartScreen	Enabled	
Prevent bypassing Windows Defender SmartScreen prompts for sites	Enabled	

Windows Components/OneDrive hide

Policy	Setting	Comment
Prevent the usage of OneDrive for file storage	Enabled	

Windows Components/Remote Desktop Services/Remote Desktop Connection Client hide

Policy	Setting	Comment
Do not allow passwords to be saved	Enabled	

Windows Components/Remote Desktop Services/Remote Desktop Session Host/Device and Resource Redirection hide

Policy	Setting	Comment
Do not allow drive redirection	Enabled	

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

Policy	Setting	Comment
Always prompt for password upon connection	Enabled	
Require secure RPC communication	Enabled	
Require use of specific security layer for remote (RDP) connections	Enabled	

Security Layer	SSL
Choose the security layer from the drop-down list.	

Policy	Setting	Comment
Require user authentication for remote connections by using Network Level Authentication	Enabled	
Set client connection encryption level	Enabled	

Encryption Level	High Level
Choose the encryption level from the drop-down list.	

Windows Components/Remote Desktop Services/Remote Desktop Session Host/Session Time Limits hide

Policy	Setting	Comment
End session when time limits are reached	Enabled	

Windows Components/Remote Desktop Services/Remote Desktop Session Host/Temporary folders hide

Policy	Setting	Comment
Do not delete temp folders upon exit	Disabled	
Do not use temporary folders per session	Disabled	

Windows Components/RSS Feeds hide

Policy	Setting	Comment
Prevent downloading of enclosures	Enabled	

Windows Components/Search hide

Policy	Setting	Comment
Allow indexing of encrypted files	Disabled	
Allow search and Cortana to use location	Disabled	

Windows Components/Store hide

Policy	Setting	Comment
Turn off Automatic Download and Install of updates	Disabled	
Turn off the offer to update to the latest version of Windows	Enabled	

Windows Components/Text Input hide

Policy	Setting	Comment
Improve inking and typing recognition	Disabled	

Windows Components/Windows Defender SmartScreen/Explorer hide

Policy	Setting	Comment
Configure Windows Defender SmartScreen	Enabled	

Pick one of the following settings:	Warn and prevent bypass

Windows Components/Windows Game Recording and Broadcasting

Policy	Setting	Comment
Enables or disables Windows Game Recording and Broadcasting	Disabled	

Windows Components/Windows Ink Workspace hide

Policy	Setting	Comment
Allow Windows Ink Workspace	Enabled	
Choose one of the following actions		

Windows Components/Windows Installer hide

Policy	Setting	Comment
Allow user control over installs	Disabled	
Always install with elevated privileges	Disabled	

Windows Components/Windows Logon Options hide

Policy	Setting	Comment
Sign-in and lock last interactive user automatically after a restart	Disabled	

Windows Components/Windows PowerShell hide

Policy	Setting	Comment
Turn on Script Execution	Enabled	
Execution Policy	Allow local scripts and remote signed scripts	

Windows Components/Windows Remote Management (WinRM)/WinRM Client hide

Policy	Setting	Comment
Allow Basic authentication	Disabled	
Allow unencrypted traffic	Disabled	
Disallow Digest authentication	Enabled	

Windows Components/Windows Remote Management (WinRM)/WinRM Service hide

Policy	Setting	Comment
Allow Basic authentication	Disabled	
Allow unencrypted traffic	Disabled	
Disallow WinRM from storing RunAs credentials	Enabled	

Windows Components/Windows Security/App and browser protection hide

Policy	Setting	Comment
Prevent users from modifying settings	Enabled	

Windows Components/Windows Update/Legacy Policies hide

Policy	Setting	Comment

No auto-restart with logged on users for scheduled automatic updates installations	Disabled

Windows Components/Windows Update/Manage end user experience hide

Policy	Setting	Comment
Configure Automatic Updates	Enabled	

Configure automatic updating:	4 - Auto download and schedule the install
The following settings are only required and applicable if 4 is selected.	
Install during automatic maintenance	Disabled
Scheduled install day:	0 - Every day
Scheduled install time:	03:00
If you have selected "4 – Auto download and schedule the install" for your scheduled install day and specified a schedule, you also have the option to limit updating to a weekly, bi-weekly or monthly occurrence, using the options below:	
Every week	Enabled
First week of the month	Disabled
Second week of the month	Disabled
Third week of the month	Disabled
Fourth week of the month	Disabled
Install updates for other Microsoft products	Disabled

Policy	Setting	Comment
Remove access to "Pause updates" feature	Enabled	

Preferences hide

Windows Settings hide

Registry hide

AllowGameDVR (Order: 1) hide

General hide

Action	Update

Properties

Hive	HKEY_LOCAL_MACHINE
Key path	SOFTWARE\Policies\Microsoft\Windows\GameDVR\
Value name	AllowGameDVR
Value type	REG_DWORD
Value data	0x0 (0)

Common hide

Options

Stop processing items on this extension if an error occurs on this item	No
Remove this item when it is no longer applied	No
Apply once and do not reapply	No

User Configuration (Enabled) hide

No settings defined.