

ID	Einstellungsname	Optionen	Empfohlene Einstellung	BSI referenzierte Maßnahme
1.	Prevent OneDrive files from syncing over metered connections		Enabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
		Metered Network Setting	Block syncing on all metered connections	
2.	Prevent the usage of OneDrive for file storage		Enabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
3.	Turn off the Store application		Enabled	M 2.32 Einrichtung einer eingeschränkten Benutzerumgebung <a href="https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02032.html">https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02032.html</a>
4.	Do not sync Apps		Enabled	M 2.32 Einrichtung einer eingeschränkten Benutzerumgebung <a href="https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02032.html">https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02032.html</a>
		Allow users to turn "AppSync" syncing on.	FALSCH	
5.	Allow development of Windows Store apps without installing a developer license		Not Configured	M 2.32 Einrichtung einer eingeschränkten Benutzerumgebung <a href="https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02032.html">https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02032.html</a>
6.	Turn on dynamic Content URI Rules for Windows store apps		Not Configured	M 2.32 Einrichtung einer eingeschränkten Benutzerumgebung <a href="https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02032.html">https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02032.html</a>
		Content URI Rules:		
7.	WDigest Authentication (disabling may require KB2871997)		Disabled	M 2.32 Einrichtung einer eingeschränkten Benutzerumgebung <a href="https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02032.html">https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02032.html</a>

ID	Einstellungsname	Optionen	Empfohlene Einstellung	BSI referenzierte Maßnahme
8.	Apply UAC restrictions to local accounts on network logons		Enabled	M 2.32 Einrichtung einer eingeschränkten Benutzerumgebung <a href="https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02032.html">https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02032.html</a>
9.	Allow antimalware service to remain running always		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
10.	Allow antimalware service to startup with normal priority		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
11.	Allow definition updates from Microsoft Update		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
12.	Allow definition updates when running on battery power		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
13.	Allow notifications to disable definitions based reports to Microsoft MAPS		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
14.	Allow real-time definition updates based on reports to Microsoft MAPS		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
15.	Allow users to pause scan		Disabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
16.	Always automatically restart at the scheduled time		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
		work (minutes):		
17.	Check for the latest virus and spyware definitions before running a scheduled scan		Enabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
18.	Check for the latest virus and spyware definitions on startup		Enabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen

ID	Einstellungsname	Optionen	Empfohlene Einstellung	BSI referenzierte Maßnahme
19.	Configure local setting override for maximum percentage of CPU utilization		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
20.	Configure local setting override for monitoring file and program activity on your computer		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
21.	Configure local setting override for monitoring for incoming and outgoing file activity		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
22.	Configure local setting override for reporting to Microsoft MAPS		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
23.	Configure local setting override for scanning all downloaded files and attachments		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
24.	Configure local setting override for schedule scan day		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
25.	Configure local setting override for scheduled quick scan time		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
26.	Configure local setting override for scheduled scan time		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
27.	Configure local setting override for the removal of items from Quarantine folder		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
28.	Configure local setting override for the scan type to use for a scheduled scan		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
29.	Configure local setting override for the time of day to run a scheduled full scan to complete remediation		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
30.	Configure local setting override for turn on behavior monitoring		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen

ID	Einstellungsname	Optionen	Empfohlene Einstellung	BSI referenzierte Maßnahme
31.	Configure local setting override to turn off Intrusion Prevention System		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
32.	Configure local setting override to turn on real-time protection		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
33.	Configure monitoring for incoming and outgoing file and program activity		Enabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
		Configure monitoring for incoming and outgoing file and program activity	bi-directional (full on-access)	
34.	Configure removal of items from Quarantine folder		Enabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
		Configure removal of items from Quarantine folder	7	
35.	Configure time out for detections in critically failed state		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
		Configure time out for detections in critically failed state		
36.	Configure time out for detections in non-critical failed state		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
		Configure time out for detections in non-critical failed state		
37.	Configure time out for detections in recently remediated state		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
		Configure time out for detections in recently remediated state		
38.	Configure time out for detections requiring		Not Configured	M 4.244 Sichere Systemkonfiguration von

ID	Einstellungsname	Optionen	Empfohlene Einstellung	BSI referenzierte Maßnahme
	additional action	Configure time out for detections requiring additional action		Windows Client-Betriebssystemen
39.	Configure Watson events		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
40.	Configure Windows software trace preprocessor components	Configure Windows software trace preprocessor components	Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
41.	Configure WPP tracing level		Enabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
		Configure WPP tracing level	1	
42.	Create a system restore point		Enabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
43.	Define file shares for downloading definition updates		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
		Define file shares for downloading definition updates		
44.	Define the maximum size of downloaded files and attachments to be scanned		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
		Define the maximum size of downloaded files and attachments to be scanned		
45.	Define the number of days after which a catch-up		Not Configured	M 4.244 Sichere Systemkonfiguration von

ID	Einstellungsname	Optionen	Empfohlene Einstellung	BSI referenzierte Maßnahme
	definition update is required	Define the number of days after which a catch-up definition update is required		Windows Client-Betriebssystemen
46.	Define the number of days before spyware definitions are considered out of date		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
		Define the number of days before spyware definitions are considered out of date		
47.	Define the number of days before virus definitions are considered out of date		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
		Define the number of days before virus definitions are considered out of date		
48.	Define the order of sources for downloading definition updates		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
		Define the order of sources for downloading definition updates		
49.	Define the rate of detection events for logging		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
		Define the rate of detection events for logging		
50.	Display additional text to clients when they need to		Not Configured	M 4.244 Sichere Systemkonfiguration von

ID	Einstellungsname	Optionen	Empfohlene Einstellung	BSI referenzierte Maßnahme
	perform an action	Display additional text to clients when they need to perform an action		Windows Client-Betriebssystemen
51.	Display notifications to clients when they need to perform actions		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
52.	Enable LSA Protection		Enabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
53.	Extension Exclusions		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
		Extension Exclusions		
54.	Initiate definition update on startup		Enabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
55.	IP address range Exclusions		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
		IP address range Exclusions		
56.	Lsass.exe audit mode		Enabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
57.	Monitor file and program activity on your computer		Enabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
58.	Path Exclusions		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
		Path Exclusions		
59.	Port number Exclusions		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
		Port number Exclusions		
60.	Process Exclusions		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
		Process Exclusions		
61.	Process Exclusions for outbound traffic		Not Configured	M 4.244 Sichere Systemkonfiguration von

ID	Einstellungsname	Optionen	Empfohlene Einstellung	BSI referenzierte Maßnahme
		Process Exclusions for outbound traffic		Windows Client-Betriebssystemen
62.	Randomize scheduled task times		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
63.	Run full scan on mapped network drives		Enabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
64.	Scan all downloaded files and attachments		Enabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
65.	Scan archive files		Enabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
66.	Scan network files		Enabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
67.	Scan packed executables		Enabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
68.	Scan removable drives		Enabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
69.	Specify additional definition sets for network traffic inspection		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
		Specify additional definition sets for network traffic inspection		
70.	Specify the day of the week to check for definition updates		Enabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
		Specify the day of the week to check for definition updates	Every Day	
71.	Specify the day of the		Enabled	M 4.244 Sichere



ID	Einstellungsname	Optionen	Empfohlene Einstellung	BSI referenzierte Maßnahme
	week to run a scheduled full scan to complete remediation	Specify the day of the week to run a scheduled full scan to complete remediation	Every Day	Systemkonfiguration von Windows Client-Betriebssystemen
72.	Specify the day of the week to run a scheduled scan		Enabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
		Specify the day of the week to run a scheduled scan	Friday	
73.	Specify the interval to check for definition updates		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
		Specify the interval to check for definition updates		
74.	Specify the interval to run quick scans per day		Enabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
		Specify the interval to run quick scans per day	4	
75.	Specify the maximum depth to scan archive files		Enabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
		Specify the maximum depth to scan archive files	5	
76.	Specify the maximum percentage of CPU utilization during a scan		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
		Specify the maximum percentage of CPU utilization during a scan		
77.	Specify the maximum size of archive files to be scanned		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
		Specify the maximum size of archive files to be scanned		
78.	Specify the scan type to use for a scheduled scan		Not Configured	M 4.244 Sichere Systemkonfiguration von

ID	Einstellungsname	Optionen	Empfohlene Einstellung	BSI referenzierte Maßnahme
		Specify the scan type to use for a scheduled scan		Windows Client-Betriebssystemen
79.	Specify the time for a daily quick scan		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
		Specify the time for a daily quick scan		
80.	Specify the time of day to run a scheduled full scan to complete remediation		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
		Specify the time of day to run a scheduled full scan to complete remediation		
81.	Specify the time of day to run a scheduled scan		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
		Specify the time of day to run a scheduled scan		
82.	Specify the time to check for definition updates		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
		Specify the time to check for definition updates		
83.	Specify threat alert levels at which default action should not be taken when detected		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
		Specify threat alert levels at which default action should not be taken when detected		
84.	Specify threats upon which default action		Not Configured	M 4.244 Sichere Systemkonfiguration von

ID	Einstellungsname	Optionen	Empfohlene Einstellung	BSI referenzierte Maßnahme
	should not be taken when detected	Specify threats upon which default action should not be taken when detected		Windows Client-Betriebssystemen
85.	Start the scheduled scan only when computer is on but not in use		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
86.	Threat ID Exclusions		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
		Threat ID Exclusions		
87.	Turn off downloading of print drivers over HTTP		Enabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
88.	Turn on behavior monitoring		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
89.	Turn on catch-up full scan		Enabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
90.	Turn on catch-up quick scan		Enabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
91.	Turn on definition retirement		Enabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
92.	Turn on e-mail scanning		Enabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
93.	Turn on heuristics		Enabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
94.	Turn on Information Protection Control		Enabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen

ID	Einstellungsname	Optionen	Empfohlene Einstellung	BSI referenzierte Maßnahme
95.	Turn on network protection against exploits of known vulnerabilities		Enabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
96.	Turn on process scanning whenever real-time protection is enabled		Enabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
97.	Turn on protocol recognition		Enabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
98.	Turn on raw volume write notifications		Enabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
99.	Turn on removal of items from scan history folder		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
		Turn on removal of items from scan history folder		
100.	Turn on reparse point scanning		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
101.	Turn on scan after signature update		Enabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
102.	Default Action and Mitigation Settings		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
		Anti Detours:		
		Banned Functions:		
		Deep Hooks:		
		Exploit Action:		
103.	Application Configuration		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
		Application		
104.	Default Protections for Internet Explorer		Enabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen

ID	Einstellungsname	Optionen	Empfohlene Einstellung	BSI referenzierte Maßnahme
105	Default Protections for Popular Software		Enabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
106	Default Protections for Recommended Software		Enabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
107	Configure local administrator merge behavior for lists		Disabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen
108	Define addresses to bypass proxy server		Not Configured	M 2.32 Einrichtung einer eingeschränkten Benutzerumgebung <a href="https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02032.html">https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02032.html</a>
		Define addresses to bypass proxy server		
109	Define proxy server for connecting to the network		Not Configured	M 2.32 Einrichtung einer eingeschränkten Benutzerumgebung <a href="https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02032.html">https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02032.html</a>
		Define proxy server for connecting to the network		
110	Do not connect to any Windows Update Internet locations		Enabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen