

UNCLASSIFIED



MICROSOFT (MS) DEFENDER ANTIVIRUS STIG REVISION HISTORY

Version 2, Release 10

30 September 2026

Developed by DISA for the DoW

UNCLASSIFIED

REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
V2R10	Microsoft Defender Antivirus STIG, V2R9	- WNDF-AV-000001, WNDF-AV-000018, WNDF-AV-000019, WNDF-AV-000020, WNDF-AV-000021, WNDF-AV-000022, WNDF-AV-000024, WNDF-AV-000025, WNDF-AV-000026, WNDF-AV-000031, WNDF-AV-000027, WNDF-AV-000039 - Added Intune registry location to check. - Requirements were updated throughout to reflect the change from DOD to DoW.	30 September 2026
V2R9	Microsoft Defender Antivirus STIG, V2R8	- WNDF-AV-000005, WNDF-AV-000006, WNDF-AV-000007 - Added note that setting WNDF-AV-000100 will hide this registry value. - WNDF-AV-000054 - Changed STIGID to WNDF-AV-000100 to be the last line in the STIG. Added note to Check. - Rule numbers updated throughout due to changes in the content management system.	01 July 2026
V2R8	- Microsoft Windows Defender AV STIG, V2R7	- WNDF-AV-000004, WNDF-AV-000005, WNDF-AV-000006, WNDF-AV-000007, WNDF-AV-000009, WNDF-AV-000012, WNDF-AV-000017, WNDF-AV-000018, WNDF-AV-000019, WNDF-AV-000021, WNDF-AV-000023, WNDF-AV-000024, WNDF-AV-000028, WNDF-AV-000029 - Updated CCI to Rev 5 Control. - WNDF-AV-000043, WNDF-AV-000044, WNDF-AV-000045, WNDF-AV-000046, WNDF-AV-000050, WNDF-AV-000051, WNDF-AV-000052, WNDF-AV-000054, WNDF-AV-000056, WNDF-AV-000057, WNDF-AV-000058, WNDF-AV-000070, WNDF-AV-000071, WNDF-AV-000073 - Removed "OK" and "Apply" from Fix. - WNDF-AV-000047, WNDF-AV-000048, WNDF-AV-000049 - Changed rule title to state "audit". Removed "OK" and "Apply" from Fix. - WNDF-AV-000055, WNDF-AV-000064, WNDF-AV-000065, WNDF-AV-000072, WNDF-AV-000076, WNDF-AV-000077 - Updated CCI to Rev. 5 control. Removed "OK" and "Apply" from Fix.	01 April 2026

REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
		- WNDF-AV-000068 - Added NA statement for desktops. Removed OK and Apply from Fix. - WNDF-AV-000074, WNDF-AV-000075 - Corrected fix path. Removed “OK” and “Apply” from Fix.	
V2R7	- Microsoft Windows Defender AV STIG, V2R6 - Microsoft Windows Defender AV Overview	- WNDF-AV-000054 - Changed registry value reference from “HideExclusionsFromLocalUsers” to “HideExclusionsFromLocalAdmins”. - WNDF-AV-000069 - Removed duplicate requirement. - Updated verbiage in Overview section 3.	05 January 2026
V2R6	- Microsoft Windows Defender AV STIG, V2R5	- Rule numbers updated throughout due to changes in the content management system. - WNDF-AV-000018 - Altered setting from disabled to enabled. - WNDF-AV-000043, WNDF-AV-000044, WNDF-AV-000045, WNDF-AV-000046, WNDF-AV-000050, WNDF-AV-000051, WNDF-AV-000052, WNDF-AV-000054, WNDF-AV-000055, WNDF-AV-000056, WNDF-AV-000057, WNDF-AV-000058, WNDF-AV-000064, WNDF-AV-000065, WNDF-AV-000069, WNDF-AV-000070, WNDF-AV-000071, WNDF-AV-000072, WNDF-AV-000073, WNDF-AV-000074, WNDF-AV-000075, WNDF-AV-000076, WNDF-AV-000077 - Added registry path to check. - WNDF-AV-000047, WNDF-AV-000048, WNDF-AV-000049 - Altered setting from block to audit. Added registry path to check. - WNDF-AV-000053, WNDF-AV-000059, WNDF-AV-000060, WNDF-AV-000061, WNDF-AV-000062, WNDF-AV-000063, WNDF-AV-000066, WNDF-AV-000067 - Removed duplicate requirement. - WNDF-AV-000068 - Altered typo in check path. Added registry path to check.	24 September 2025
V2R5	- Microsoft Windows	- Rule numbers updated throughout due to changes in the content management system.	20 August 2025

REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
	Defender AV STIG, V2R4	- WNDF-AV-000010 - Altered to allow a value of 1 or 2. - WNDF-AV-000043 - Added requirement to block Adobe Reader from creating child processes. - WNDF-AV-000044 - Added requirement to block credential stealing from the Windows local security authority subsystem. - WNDF-AV-000045 - Added requirement to block untrusted and unsigned processes that run from USB. - WNDF-AV-000046 - Added requirement to use advanced protection against ransomware. - WNDF-AV-000047 - Added requirement to block process creations originating from PSEXEC and WMI commands. - WNDF-AV-000048 - Added requirement to block persistence through WMI event subscription. - WNDF-AV-000049 - Added requirement to block executable files from running unless they meet a prevalence, age, or trusted list criterion. - WNDF-AV-000050 - Added requirement to block Office communication application from creating child processes. - WNDF-AV-000051 - Added requirement to block abuse of exploited vulnerable signed drivers. - WNDF-AV-000052 - Added requirement to configure local administrator merge behavior for lists. - WNDF-AV-000053 - Added requirement to enable routine remediation. - WNDF-AV-000054 - Added requirement to control whether exclusions are visible to Local Admins. - WNDF-AV-000055 - Added requirement to randomize scheduled task times. - WNDF-AV-000056 - Added requirement to hide the Family options area.	

REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
		- WNDF-AV-000057 - Added requirement to enable file hash computation feature. - WNDF-AV-000058 - Added requirement to configure extended cloud check. - WNDF-AV-000059 - Added requirement to turn on behavior monitoring. - WNDF-AV-000060 - Added requirement to scan all downloaded files and attachments. - WNDF-AV-000061 - Added requirement to monitor file and program activity. - WNDF-AV-000062 - Added requirement to turn on real-time protection. - WNDF-AV-000063 - Added requirement to turn on process scanning whenever real-time protection is enabled. - WNDF-AV-000064 - Added requirement to turn on script scanning. - WNDF-AV-000065 - Added requirement to configure real-time protection and Security Intelligence Updates during OOBE. - WNDF-AV-000066 - Added requirement to configure monitoring for incoming and outgoing file and program activity. - WNDF-AV-000067 - Added requirement to configure controlled folder access. - WNDF-AV-000068 - Added requirement to control whether network protection is allowed to be configured into block or audit mode on Windows Server. - WNDF-AV-000069 - Added requirement to turn off Auto Exclusions. - WNDF-AV-000070 - Added requirement to enable EDR in block mode. - WNDF-AV-000071 - Added requirement to report Dynamic Signature dropped events. - WNDF-AV-000072 - Added requirement to scan excluded files and directories during quick scans. - WNDF-AV-000073 - Added requirement to configure cloud protection level. - WNDF-AV-000074 - Added requirement to convert warn verdict to block.	

REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
		- WNDF-AV-000075 - Added requirement to turn on asynchronous inspection. - WNDF-AV-000076 - Added requirement to scan packed executables. - WNDF-AV-000077 - Added requirement to turn on heuristics.	
V2R4	- Microsoft Windows Defender AV STIG, V2R3	- STIG title: Revised from Microsoft Windows Defender Antivirus to Microsoft Defender Antivirus. - All requirements: In all Check text, revised configuration path reference to Microsoft Defender. Revised text as needed for grammar/punctuation.	31 May 2022
V2R3	- Microsoft Windows Defender AV STIG, V2R2	- In Overview Section 2.2, removed Windows 2012 and 8.1 references. - WNDF-AV-000030 - Revised registry path: HKLM\Software\Policies\Microsoft\Windows Defender\Signature Updates.	01 November 2021
V2R2	- Microsoft Windows Defender AV STIG, V2R1	- In Overview Section 3, Applicability and Usage, revised wording and removed conflicting guidance. - WNDF-AV-000004 - Removed 2016/2019 references because operating systems were updated 15 November 2019 with AV guidance.	04 May 2021
V2R1	- Microsoft Windows Defender AV STIG, V1R9	- DISA migrated the STIG to a new content management system, which renumbered all Groups (V-numbers) and Rules (SV-numbers). With the new Group and Rule numbers, DISA incremented the version number from V1R9 to V2R1. - WNDF-AV-000005 - Added exception language into rule to allow file/folders to be excluded from scanning. - WNDF-AV-000028 - Modified check text to "third-party anti-spyware".	13 November 2020
V1R9	- Microsoft Windows Defender AV STIG, V1R8	- V-75241 - Updated Check to include NA statement if third-party spyware is installed. - V-75243 - Updated Check to include NA statement if third-party antivirus protection is installed.	15 May 2020

REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
V1R8	- Microsoft Windows Defender AV STIG, V1R7	- V-75147 - Revised requirement to configure Windows Defender AV to block Potentially Unwanted Application feature.	24 April 2020
V1R7	- Microsoft Windows Defender AV STIG, V1R6 - Microsoft Windows Defender AV Overview	- V-75153 - Corrected rule title and check content to reflect original requirement of joining Microsoft MAPs. - V-75167 - Corrected rule title and check content to reflect original requirement of joining Microsoft MAPs. - Modified Overview to include Windows Server 2019 as being subject to the Windows Defender STIG inspection.	24 January 2020
V1R6	- Microsoft Windows Defender AV STIG, V1R5	- V-75167 - Corrected back to properties for “Enabled” as the conflicting STIG ID in the Windows OS STIG has been removed.	26 July 2019
V1R5	- Microsoft Windows Defender AV STIG, V1R4	- V-75167 - Clarified requirement as it relates to the Windows Operating System and McAfee STIGS. - V-75153 - Added check and fix verbiage for both Win10 and Server 2016 versions.	26 April 2019
V1R4	- Microsoft Windows Defender AV STIG, V1R3	- Updated Overview document to add Applicability and Usage section. - V-75153 - Removed the allowance of the value “Disabled”. - V-75247 - Separated out each threat level. Modified this requirement for threat level Severe. - V-79965 - Added requirement for threat level High. - V-79967 - Added requirement for threat level Medium. - V-79971 - Added requirement for threat level Low.	27 April 2018
V1R3	- Microsoft Windows Defender AV STIG, V1R2	- V-75207 – Updated Fix Text.	26 January 2018
V1R2	- Microsoft Windows Defender AV STIG, V1R1	- V-75161 – Added NA statement for unclassified systems. - V-75163 – Added NA statement for unclassified systems.	31 October 2017

REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
		- V-75167 – Added NA statement for unclassified systems. - V-75207 – Added NA statement for unclassified systems. - V-75147 – Updated to add custom admin template information. - V-77965 – Added new requirement to block executable content from email client and webmail. - V-77967 – Added new requirement to block Office applications from creating child processes. - V-77969 – Added new requirement to block Office applications from creating executable content. - V-77971 – Added new requirement to block Office applications from injecting into other processes. - V-77973 – Added new requirement to impede JavaScript and VBScript to launch executables. - V-77975 – Added new requirement to block execution of potentially obfuscated scripts. - V-77977 – Added new requirement to block Win32 imports from macro code in Office. - V-77979 – Added new requirement to prevent user and apps from accessing dangerous websites.	
V1R1	- NA	- Initial Release.	26 July 2017