Trellix

2025-Sep-03

Trellix Policy Auditor Content Update Summary

Product / Version	Content Version
Trellix Policy Auditor 6.x	1425

New Checks

Oval ID	Title
oval:com.mcafee.oval.common:def:3014383	Google Chrome Extended Stable Channel Update 138.0.7204.243 for Windows
oval:com.mcafee.oval.common:def:3014386	Google Chrome Security Update 139.0.7258.155 for Windows
oval:com.mcafee.oval.common:def:3014389	Google Chrome Security Update 139.0.7258.128 for Windows
oval:com.mcafee.oval.common:def:3014392	Google Chrome Security Update 139.0.7258.67 for Windows
oval:com.mcafee.oval.common:def:3014395	Google Chrome Security Update 139.0.7258.139 for Windows
oval:com.mcafee.oval.common:def:3014398	Mozilla Thunderbird Security Update 140.2 for Windows
oval:com.mcafee.oval.common:def:3014401	Mozilla Thunderbird Security Update 142 for Windows
oval:com.mcafee.oval.common:def:3014404	Mozilla Thunderbird Security Update 128.14 for Windows
oval:com.mcafee.oval.common:def:3014407	Mozilla Firefox Security Update 142.0 for Windows
oval:com.mcafee.oval.common:def:3014410	Mozilla Firefox ESR Security Update 128.14 for Windows
oval:com.mcafee.oval.common:def:3014413	Mozilla Firefox ESR Security Update 140.2 for Windows
oval:com.mcafee.oval.common:def:3014416	Mozilla Firefox ESR Security Update 115.27 for Windows
oval:com.mcafee.oval:def:2970743	Mozilla Thunderbird Security Update 128.14 for Mac OS
oval:com.mcafee.oval:def:2970746	Mozilla Thunderbird Security Update 142 for Mac OS
oval:com.mcafee.oval:def:2970749	Mozilla Thunderbird Security Update 140.2 for Mac OS
oval:com.mcafee.oval:def:3014349	Mozilla Firefox ESR Security Update 140.2 for Mac OS
oval:com.mcafee.oval:def:3014352	Mozilla Firefox ESR Security Update 128.14 for Mac OS
oval:com.mcafee.oval:def:3014355	Mozilla Firefox ESR Security Update 115.27 for Mac OS
oval:com.mcafee.oval:def:3014358	Mozilla Firefox Security Update 142.0 for Mac OS
oval:com.mcafee.oval:def:3014361	Apple Safari Security Update 18.6 for Mac OS X
oval:com.mcafee.oval:def:3014365	Apple macOS 15.6 Update
oval:com.mcafee.oval:def:3014368	Apple macOS 15.6.1 Update
oval:com.mcafee.oval:def:3014371	Apple macOS 14.7.8 Update

Oval ID	Title
oval:com.mcafee.oval:def:3014374	Apple macOS 14.7.7 Update
oval:com.mcafee.oval:def:3014377	Apple macOS 13.7.7 Update
oval:com.mcafee.oval:def:3014380	Apple macOS 13.7.8 Update
oval:com.mcafee.oval:def:3014383	Google Chrome Extended Stable Channel Update 138.0.7204.243 for Windows
oval:com.mcafee.oval:def:3014386	Google Chrome Security Update 139.0.7258.155 for Windows
oval:com.mcafee.oval:def:3014389	Google Chrome Security Update 139.0.7258.128 for Windows
oval:com.mcafee.oval:def:3014392	Google Chrome Security Update 139.0.7258.67 for Windows
oval:com.mcafee.oval:def:3014395	Google Chrome Security Update 139.0.7258.139 for Windows
oval:com.mcafee.oval:def:3014398	Mozilla Thunderbird Security Update 140.2 for Windows is installed or not
oval:com.mcafee.oval:def:3014401	Mozilla Thunderbird Security Update 142 for Windows is installed or not
oval:com.mcafee.oval:def:3014404	Mozilla Thunderbird Security Update 128.14 for Windows is installed or not
oval:com.mcafee.oval:def:3014407	Mozilla Firefox Security Update 142.0 for Windows is installed or not
oval:com.mcafee.oval:def:3014410	Mozilla Firefox ESR Security Update 128.14 for Windows is installed or not
oval:com.mcafee.oval:def:3014413	Mozilla Firefox ESR Security Update 140.2 for Windows is installed or not
oval:com.mcafee.oval:def:3014416	Mozilla Firefox ESR Security Update 115.27 for Windows is installed or not
oval:com.mcafee.oval:def:3014419	2021-08 Servicing stack update for Windows Server 2019 (KB5005112)
oval:mil.disa.stig.defs:def:220961	The Change the system time user right must only be assigned to Administrators and Local Service and NT SERVICE\autotimesvc.
oval:mil.disa.stig.defs:def:248774	Successful/unsuccessful uses of the "rmdir" command in the operating system must generate an audit record.
oval:mil.disa.stig.defs:def:258129	The operating system operating systems must require authentication upon booting into rescue mode.
oval:mil.disa.stig.defs:def:260487	The operating system library directories must have mode 0755 or less permissive.
oval:mil.disa.stig.ubuntu2004os:def:238208	UBTU-20-010014 - The Ubuntu operating system must require users to reauthenticate for privilege escalation or when changing roles.
oval:mil.disa.stig.windows10:def:220956	WN10-UR-000005 - The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.
oval:mil.disa.stig.windows10:def:220957	WN10-UR-000010 - The Access this computer from the network user right must only be assigned to the Administrators and Remote Desktop Users groups.
oval:mil.disa.stig.windows10:def:220958	WN10-UR-000015 - The Act as part of the operating system user right must not be assigned to any groups or accounts.
oval:mil.disa.stig.windows10:def:220959	WN10-UR-000025 - The Allow log on locally user right must only be assigned to the Administrators and Users groups.
oval:mil.disa.stig.windows10:def:220960	WN10-UR-000030 - The Back up files and directories user right must only be assigned to the Administrators group.
oval:mil.disa.stig.windows10:def:220961	WN10-UR-000035 - The Change the system time user right must only be assigned to Administrators and Local Service and NT SERVICE\autotimesvc.
oval:mil.disa.stig.windows10:def:220962	WN10-UR-000040 - The Create a pagefile user right must only be assigned to the Administrators group.

Oval ID	Title
oval:mil.disa.stig.windows10:def:220963	WN10-UR-000045 - The Create a token object user right must not be assigned to any groups or accounts.
oval:mil.disa.stig.windows10:def:220964	WN10-UR-000050 - The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.
oval:mil.disa.stig.windows10:def:220965	WN10-UR-000055 - The Create permanent shared objects user right must not be assigned to any groups or accounts.
oval:mil.disa.stig.windows10:def:220966	WN10-UR-000060 - The Create symbolic links user right must only be assigned to the Administrators group.
oval:mil.disa.stig.windows10:def:220967	WN10-UR-000065 - The Debug programs user right must only be assigned to the Administrators group.
oval:mil.disa.stig.windows10:def:220968	WN10-UR-000070 - The Deny access to this computer from the network user right on workstations must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems and unauthenticated access on all systems.
oval:mil.disa.stig.windows10:def:220969	WN10-UR-000075 - The "Deny log on as a batch job" user right on domain-joined workstations must be configured to prevent access from highly privileged domain accounts.
oval:mil.disa.stig.windows10:def:220971	WN10-UR-000085 - The Deny log on locally user right on workstations must be configured to prevent access from highly privileged domain accounts on domain systems and unauthenticated access on all systems.
oval:mil.disa.stig.windows10:def:220972	WN10-UR-000090 - The Deny log on through Remote Desktop Services user right on Windows 10 workstations must at a minimum be configured to prevent access from highly privileged domain accounts and local accounts on domain systems and unauthenticated access on all systems.
oval:mil.disa.stig.windows10:def:220973	WN10-UR-000095 - The Enable computer and user accounts to be trusted for delegation user right must not be assigned to any groups or accounts.
oval:mil.disa.stig.windows10:def:220974	WN10-UR-000100 - The Force shutdown from a remote system user right must only be assigned to the Administrators group.
oval:mil.disa.stig.windows10:def:220975	WN10-UR-000110 - The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.
oval:mil.disa.stig.windows10:def:220976	WN10-UR-000120 - The Load and unload device drivers user right must only be assigned to the Administrators group.
oval:mil.disa.stig.windows10:def:220977	WN10-UR-000125 - The Lock pages in memory user right must not be assigned to any groups or accounts.
oval:mil.disa.stig.windows10:def:220978	WN10-UR-000130 - The Manage auditing and security log user right must only be assigned to the Administrators group.
oval:mil.disa.stig.windows10:def:220979	WN10-UR-000140 - The Modify firmware environment values user right must only be assigned to the Administrators group.
oval:mil.disa.stig.windows10:def:220981	WN10-UR-000150 - The Profile single process user right must only be assigned to the Administrators group.
oval:mil.disa.stig.windows10:def:220982	WN10-UR-000160 - The Restore files and directories user right must only be assigned to the Administrators group.
oval:mil.disa.stig.windows10:def:220983	WN10-UR-000165 - The Take ownership of files or other objects user right must only be assigned to the Administrators group.
oval:mil.disa.stig.windows2019:def:205643	WN19-UR-000170 - Windows Server 2019 Manage auditing and security log user right must only be assigned to the Administrators group.

Oval ID	Title
oval:mil.disa.stig.windows2019:def:205665	WN19-DC-000340 - Windows Server 2019 Access this computer from the network user right must only be assigned to the Administrators, Authenticated Users, and Enterprise Domain Controllers groups on domain controllers.
oval:mil.disa.stig.windows2019:def:205666	WN19-DC-000360 - Windows Server 2019 Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group on domain controllers.
oval:mil.disa.stig.windows2019:def:205667	WN19-DC-000370 - Windows Server 2019 Deny access to this computer from the network user right on domain controllers must be configured to prevent unauthenticated access.
oval:mil.disa.stig.windows2019:def:205668	WN19-DC-000380 - Windows Server 2019 Deny log on as a batch job user right on domain controllers must be configured to prevent unauthenticated access.
oval:mil.disa.stig.windows2019:def:205669	WN19-DC-000390 - Windows Server 2019 Deny log on as a service user right must be configured to include no accounts or groups (blank) on domain controllers.
oval:mil.disa.stig.windows2019:def:205670	WN19-DC-000400 - Windows Server 2019 Deny log on locally user right on domain controllers must be configured to prevent unauthenticated access.
oval:mil.disa.stig.windows2019:def:205671	WN19-MS-000070 - Windows Server 2019 "Access this computer from the network" user right must only be assigned to the Administrators and Authenticated Users groups on domain-joined member servers and standalone or nondomain-joined systems.
oval:mil.disa.stig.windows2019:def:205672	WN19-MS-000080 - Windows Server 2019 "Deny access to this computer from the network" user right on domain-joined member servers must be configured to prevent access from highly privileged domain accounts and local accounts and from unauthenticated access on all systems.
oval:mil.disa.stig.windows2019:def:205673	WN19-MS-000090 - Windows Server 2019 "Deny log on as a batch job" user right on domain-joined member servers must be configured to prevent access from highly privileged domain accounts and from unauthenticated access on all systems.
oval:mil.disa.stig.windows2019:def:205675	WN19-MS-000110 - Windows Server 2019 "Deny log on locally" user right on domain-joined member servers must be configured to prevent access from highly privileged domain accounts and from unauthenticated access on all systems.
oval:mil.disa.stig.windows2019:def:205676	WN19-UR-000030 - Windows Server 2019 Allow log on locally user right must only be assigned to the Administrators group.
oval:mil.disa.stig.windows2019:def:205732	WN19-DC-000410 - Windows Server 2019 Deny log on through Remote Desktop Services user right on domain controllers must be configured to prevent unauthenticated access.
oval:mil.disa.stig.windows2019:def:205733	WN19-MS-000120 - Windows Server 2019 "Deny log on through Remote Desktop Services" user right on domain-joined member servers must be configured to prevent access from highly privileged domain accounts and all local accounts and from unauthenticated access on all systems.
oval:mil.disa.stig.windows2019:def:205744	WN19-DC-000350 - Windows Server 2019 Add workstations to domain user right must only be assigned to the Administrators group on domain controllers.
oval:mil.disa.stig.windows2019:def:205745	WN19-DC-000420 - Windows Server 2019 Enable computer and user accounts to be trusted for delegation user right must only be assigned to the Administrators group on domain controllers.
oval:mil.disa.stig.windows2019:def:205748	WN19-MS-000130 - Windows Server 2019 "Enable computer and user accounts to be trusted for delegation" user right must not be assigned to any groups or accounts on domain-joined member servers and standalone or nondomain-joined systems.
oval:mil.disa.stig.windows2019:def:205749	WN19-UR-000010 - Windows Server 2019 Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.

Oval ID	Title
oval:mil.disa.stig.windows2019:def:205750	WN19-UR-000020 - Windows Server 2019 Act as part of the operating system user right must not be assigned to any groups or accounts.
oval:mil.disa.stig.windows2019:def:205751	WN19-UR-000040 - Windows Server 2019 Back up files and directories user right must only be assigned to the Administrators group.
oval:mil.disa.stig.windows2019:def:205752	WN19-UR-000050 - Windows Server 2019 Create a pagefile user right must only be assigned to the Administrators group.
oval:mil.disa.stig.windows2019:def:205753	WN19-UR-000060 - Windows Server 2019 Create a token object user right must not be assigned to any groups or accounts.
oval:mil.disa.stig.windows2019:def:205754	WN19-UR-000070 - Windows Server 2019 Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.
oval:mil.disa.stig.windows2019:def:205755	WN19-UR-000080 - Windows Server 2019 Create permanent shared objects user right must not be assigned to any groups or accounts.
oval:mil.disa.stig.windows2019:def:205756	WN19-UR-000090 - Windows Server 2019 Create symbolic links user right must only be assigned to the Administrators group.
oval:mil.disa.stig.windows2019:def:205757	WN19-UR-000100 - Windows Server 2019 Debug programs: user right must only be assigned to the Administrators group.
oval:mil.disa.stig.windows2019:def:205758	WN19-UR-000110 - Windows Server 2019 Force shutdown from a remote system user right must only be assigned to the Administrators group.
oval:mil.disa.stig.windows2019:def:205759	WN19-UR-000120 - Windows Server 2019 Generate security audits user right must only be assigned to Local Service and Network Service.
oval:mil.disa.stig.windows2019:def:205760	WN19-UR-000130 - Windows Server 2019 Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.
oval:mil.disa.stig.windows2019:def:205761	WN19-UR-000140 - Windows Server 2019 Increase scheduling priority: user right must only be assigned to the Administrators group.
oval:mil.disa.stig.windows2019:def:205762	WN19-UR-000150 - Windows Server 2019 Load and unload device drivers user right must only be assigned to the Administrators group.
oval:mil.disa.stig.windows2019:def:205763	WN19-UR-000160 - Windows Server 2019 Lock pages in memory user right must not be assigned to any groups or accounts.
oval:mil.disa.stig.windows2019:def:205764	WN19-UR-000180 - Windows Server 2019 Modify firmware environment values user right must only be assigned to the Administrators group.
oval:mil.disa.stig.windows2019:def:205766	WN19-UR-000200 - Windows Server 2019 Profile single process user right must only be assigned to the Administrators group.
oval:mil.disa.stig.windows2019:def:205767	WN19-UR-000210 - Windows Server 2019 Restore files and directories user right must only be assigned to the Administrators group.
oval:mil.disa.stig.windows2019:def:205768	WN19-UR-000220 - Windows Server 2019 Take ownership of files or other objects user right must only be assigned to the Administrators group.

Updated Checks

Oval ID	Title
oval:mil.disa.stig.windows11:def:253254	WN11-00-000005 - Domain-joined systems must use Windows 11 Enterprise Edition 64-bit version.
oval:mil.disa.stig.defs:def:253254	Domain-joined systems must use Windows Enterprise Edition 64-bit version.

Oval ID	Title
oval:mil.disa.stig.windows11:def:253259	WN11-00-000030 - Windows 11 information systems must use BitLocker to encrypt all disks to protect the confidentiality and integrity of all information at rest.
oval:mil.disa.stig.defs:def:253259	Windows information systems must use BitLocker to encrypt all disks to protect the confidentiality and integrity of all information at rest.
oval:mil.disa.stig.windows11:def:253260	WN11-00-000031 - Windows 11 systems must use a BitLocker PIN for pre-boot authentication.
oval:mil.disa.stig.defs:def:253260	Windows systems must use a BitLocker PIN for pre-boot authentication.
oval:mil.disa.stig.windows11:def:253261	WN11-00-000032 - Windows 11 systems must use a BitLocker PIN with a minimum length of six digits for pre-boot authentication.
oval:mil.disa.stig.defs:def:253261	Windows systems must use a BitLocker PIN with a minimum length of six digits for pre-boot authentication.
oval:mil.disa.stig.windows11:def:253263	WN11-00-000040 - Windows 11 systems must be maintained at a supported servicing level.
oval:mil.disa.stig.defs:def:253263	Windows systems must be maintained at a supported servicing level.
oval:mil.disa.stig.windows11:def:253265	WN11-00-000050 - Local volumes must be formatted using NTFS.
oval:mil.disa.stig.defs:def:253265	Local volumes must be formatted using NTFS.
oval:mil.disa.stig.windows11:def:253275	WN11-00-000100 - Internet Information System (IIS) or its subcomponents must not be installed on a workstation.
oval:mil.disa.stig.defs:def:253275	Internet Information System (IIS) or its subcomponents must not be installed on a workstation.
oval:mil.disa.stig.windows11:def:253277	WN11-00-000110 - Simple TCP/IP Services must not be installed on the system.
oval:mil.disa.stig.defs:def:253277	Simple TCP/IP Services must not be installed on the system.
oval:mil.disa.stig.windows11:def:253278	WN11-00-000115 - The Telnet Client must not be installed on the system.
oval:mil.disa.stig.defs:def:253278	The Telnet Client must not be installed on the system.
oval:mil.disa.stig.windows11:def:253279	WN11-00-000120 - The TFTP Client must not be installed on the system.
oval:mil.disa.stig.defs:def:253279	The TFTP Client must not be installed on the system.
oval:mil.disa.stig.windows11:def:253283	WN11-00-000145 - Data Execution Prevention (DEP) must be configured to at least OptOut.
oval:mil.disa.stig.defs:def:253283	Data Execution Prevention (DEP) must be configured to at least OptOut.
oval:mil.disa.stig.windows11:def:253284	WN11-00-000150 - Structured Exception Handling Overwrite Protection (SEHOP) must be enabled.
oval:mil.disa.stig.defs:def:253284	Structured Exception Handling Overwrite Protection (SEHOP) must be enabled.
oval:mil.disa.stig.windows11:def:253285	WN11-00-000155 - The Windows PowerShell 2.0 feature must be disabled on the system.
oval:mil.disa.stig.defs:def:253285	The Windows PowerShell 2.0 feature must be disabled on the system.
oval:mil.disa.stig.windows11:def:253286	WN11-00-000160 - The Server Message Block (SMB) v1 protocol must be disabled on the system.
oval:mil.disa.stig.defs:def:253286	The Server Message Block (SMB) v1 protocol must be disabled on the system.
oval:mil.disa.stig.defs:def:253287	The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.

Oval ID	Title
oval:mil.disa.stig.defs:def:253288	The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.
oval:mil.disa.stig.windows11:def:253287	WN11-00-000165 - The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.
oval:mil.disa.stig.windows11:def:253288	WN11-00-000170 - The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.
oval:mil.disa.stig.windows11:def:253289	WN11-00-000175 - The Secondary Logon service must be disabled on Windows 11.
oval:mil.disa.stig.defs:def:253289	The Secondary Logon service must be disabled on Windows.
oval:mil.disa.stig.windows11:def:253297	WN11-AC-000005 - Windows 11 account lockout duration must be configured to 15 minutes or greater.
oval:mil.disa.stig.defs:def:253297	Windows account lockout duration must be configured to 15 minutes or greater.
oval:mil.disa.stig.windows11:def:253298	WN11-AC-000010 - The number of allowed bad logon attempts must be configured to three or less.
oval:mil.disa.stig.defs:def:253298	The number of allowed bad logon attempts must be configured to three or less.
oval:mil.disa.stig.windows11:def:253299	WN11-AC-000015 - The period of time before the bad logon counter is reset must be configured to 15 minutes.
oval:mil.disa.stig.defs:def:253299	The period of time before the bad logon counter is reset must be configured to 15 minutes.
oval:mil.disa.stig.windows11:def:253300	WN11-AC-000020 - The password history must be configured to 24 passwords remembered.
oval:mil.disa.stig.defs:def:253300	The password history must be configured to 24 passwords remembered.
oval:mil.disa.stig.windows11:def:253301	WN11-AC-000025 - The maximum password age must be configured to 60 days or less.
oval:mil.disa.stig.defs:def:253301	The maximum password age must be configured to 60 days or less.
oval:mil.disa.stig.windows11:def:253302	WN11-AC-000030 - The minimum password age must be configured to at least 1 day.
oval:mil.disa.stig.defs:def:253302	The minimum password age must be configured to at least 1 day.
oval:mil.disa.stig.windows11:def:253303	WN11-AC-000035 - Passwords must, at a minimum, be 14 characters.
oval:mil.disa.stig.defs:def:253303	Passwords must, at a minimum, be 14 characters.
oval:mil.disa.stig.windows11:def:253304	WN11-AC-000040 - The built-in Microsoft password complexity filter must be enabled.
oval:mil.disa.stig.defs:def:253304	The built-in Microsoft password complexity filter must be enabled.
oval:mil.disa.stig.windows11:def:253305	WN11-AC-000045 - Reversible password encryption must be disabled.
oval:mil.disa.stig.defs:def:253305	Reversible password encryption must be disabled.
oval:mil.disa.stig.windows11:def:253306	WN11-AU-000005 - The system must be configured to audit Account Logon - Credential Validation failures.
oval:mil.disa.stig.defs:def:253306	The system must be configured to audit Account Logon - Credential Validation failures.
oval:mil.disa.stig.windows11:def:253307	WN11-AU-000010 - The system must be configured to audit Account Logon - Credential Validation successes.

Oval ID	Title
oval:mil.disa.stig.defs:def:253307	The system must be configured to audit Account Logon - Credential Validation successes.
oval:mil.disa.stig.windows11:def:253308	WN11-AU-000030 - The system must be configured to audit Account Management - Security Group Management successes.
oval:mil.disa.stig.defs:def:253308	The system must be configured to audit Account Management - Security Group Management successes.
oval:mil.disa.stig.windows11:def:253309	WN11-AU-000035 - The system must be configured to audit Account Management - User Account Management failures.
oval:mil.disa.stig.defs:def:253309	The system must be configured to audit Account Management - User Account Management failures.
oval:mil.disa.stig.windows11:def:253310	WN11-AU-000040 - The system must be configured to audit Account Management - User Account Management successes.
oval:mil.disa.stig.defs:def:253310	The system must be configured to audit Account Management - User Account Management successes.
oval:mil.disa.stig.windows11:def:253312	WN11-AU-000050 - The system must be configured to audit Detailed Tracking - Process Creation successes.
oval:mil.disa.stig.defs:def:253312	The system must be configured to audit Detailed Tracking - Process Creation successes.
oval:mil.disa.stig.windows11:def:253313	WN11-AU-000054 - The system must be configured to audit Logon/Logoff - Account Lockout failures.
oval:mil.disa.stig.defs:def:253313	The system must be configured to audit Logon/Logoff - Account Lockout failures.
oval:mil.disa.stig.windows11:def:253315	WN11-AU-000065 - The system must be configured to audit Logon/Logoff - Logoff successes.
oval:mil.disa.stig.defs:def:253315	The system must be configured to audit Logon/Logoff - Logoff successes.
oval:mil.disa.stig.windows11:def:253316	WN11-AU-000070 - The system must be configured to audit Logon/Logoff - Logon failures.
oval:mil.disa.stig.defs:def:253316	The system must be configured to audit Logon/Logoff - Logon failures.
oval:mil.disa.stig.windows11:def:253317	WN11-AU-000075 - The system must be configured to audit Logon/Logoff - Logon successes.
oval:mil.disa.stig.defs:def:253317	The system must be configured to audit Logon/Logoff - Logon successes.
oval:mil.disa.stig.windows11:def:253318	WN11-AU-000080 - The system must be configured to audit Logon/Logoff - Special Logon successes.
oval:mil.disa.stig.defs:def:253318	The system must be configured to audit Logon/Logoff - Special Logon successes.
oval:mil.disa.stig.windows11:def:253319	WN11-AU-000081 - Windows 11 must be configured to audit Object Access - File Share failures.
oval:mil.disa.stig.defs:def:253319	Windows must be configured to audit Object Access - File Share failures.
oval:mil.disa.stig.windows11:def:253320	WN11-AU-000082 - Windows 11 must be configured to audit Object Access - File Share successes.
oval:mil.disa.stig.defs:def:253320	Windows must be configured to audit Object Access - File Share successes.
oval:mil.disa.stig.windows11:def:253321	WN11-AU-000083 - Windows 11 must be configured to audit Object Access - Other Object Access Events successes.
oval:mil.disa.stig.defs:def:253321	Windows must be configured to audit Object Access - Other Object Access Events successes.

Oval ID	Title
oval:mil.disa.stig.windows11:def:253322	WN11-AU-000084 - Windows 11 must be configured to audit Object Access - Other Object Access Events failures.
oval:mil.disa.stig.defs:def:253322	Windows must be configured to audit Object Access - Other Object Access Events failures.
oval:mil.disa.stig.windows11:def:253325	WN11-AU-000100 - The system must be configured to audit Policy Change - Audit Policy Change successes.
oval:mil.disa.stig.defs:def:253325	The system must be configured to audit Policy Change - Audit Policy Change successes.
oval:mil.disa.stig.windows11:def:253326	WN11-AU-000105 - The system must be configured to audit Policy Change - Authentication Policy Change successes.
oval:mil.disa.stig.defs:def:253326	The system must be configured to audit Policy Change - Authentication Policy Change successes.
oval:mil.disa.stig.windows11:def:253327	WN11-AU-000107 - The system must be configured to audit Policy Change - Authorization Policy Change successes.
oval:mil.disa.stig.defs:def:253327	The system must be configured to audit Policy Change - Authorization Policy Change successes.
oval:mil.disa.stig.windows11:def:253328	WN11-AU-000110 - The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.
oval:mil.disa.stig.defs:def:253328	The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.
oval:mil.disa.stig.windows11:def:253329	WN11-AU-000115 - The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.
oval:mil.disa.stig.defs:def:253329	The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.
oval:mil.disa.stig.windows11:def:253330	WN11-AU-000120 - The system must be configured to audit System - IPsec Driver failures.
oval:mil.disa.stig.defs:def:253330	The system must be configured to audit System - IPsec Driver failures.
oval:mil.disa.stig.windows11:def:253331	WN11-AU-000130 - The system must be configured to audit System - Other System Events successes.
oval:mil.disa.stig.defs:def:253331	The system must be configured to audit System - Other System Events successes.
oval:mil.disa.stig.windows11:def:253332	WN11-AU-000135 - The system must be configured to audit System - Other System Events failures.
oval:mil.disa.stig.defs:def:253332	The system must be configured to audit System - Other System Events failures.
oval:mil.disa.stig.windows11:def:253333	WN11-AU-000140 - The system must be configured to audit System - Security State Change successes.
oval:mil.disa.stig.defs:def:253333	The system must be configured to audit System - Security State Change successes.
oval:mil.disa.stig.windows11:def:253334	WN11-AU-000150 - The system must be configured to audit System - Security System Extension successes.
oval:mil.disa.stig.defs:def:253334	The system must be configured to audit System - Security System Extension successes.
oval:mil.disa.stig.windows11:def:253335	WN11-AU-000155 - The system must be configured to audit System - System Integrity failures.
oval:mil.disa.stig.defs:def:253335	The system must be configured to audit System - System Integrity failures.

Oval ID	Title
oval:mil.disa.stig.windows11:def:253336	WN11-AU-000160 - The system must be configured to audit System - System Integrity successes.
oval:mil.disa.stig.defs:def:253336	The system must be configured to audit System - System Integrity successes.
oval:mil.disa.stig.windows11:def:253337	WN11-AU-000500 - The Application event log size must be configured to 32768 KB or greater.
oval:mil.disa.stig.defs:def:253337	The Application event log size must be configured to 32768 KB or greater.
oval:mil.disa.stig.windows11:def:253338	WN11-AU-000505 - The Security event log size must be configured to 1024000 KB or greater.
oval:mil.disa.stig.defs:def:253338	The Security event log size must be configured to 1024000 KB or greater.
oval:mil.disa.stig.windows11:def:253339	WN11-AU-000510 - The System event log size must be configured to 32768 KB or greater.
oval:mil.disa.stig.defs:def:253339	The System event log size must be configured to 32768 KB or greater.
oval:mil.disa.stig.windows11:def:253340	WN11-AU-000515 - Windows 11 permissions for the Application event log must prevent access by non-privileged accounts.
oval:mil.disa.stig.defs:def:253340	Windows permissions for the Application event log must prevent access by non-privileged accounts.
oval:mil.disa.stig.windows11:def:253341	WN11-AU-000520 - Windows 11 permissions for the Security event log must prevent access by non-privileged accounts.
oval:mil.disa.stig.defs:def:253341	Windows permissions for the Security event log must prevent access by non-privileged accounts.
oval:mil.disa.stig.windows11:def:253342	WN11-AU-000525 - Windows 11 permissions for the System event log must prevent access by non-privileged accounts.
oval:mil.disa.stig.defs:def:253342	Windows permissions for the System event log must prevent access by non-privileged accounts.
oval:mil.disa.stig.windows11:def:253343	WN11-AU-000550 - Windows 11 must be configured to audit Other Policy Change Events Successes.
oval:mil.disa.stig.defs:def:253343	Windows must be configured to audit Other Policy Change Events Successes.
oval:mil.disa.stig.windows11:def:253344	WN11-AU-000555 - Windows 11 must be configured to audit Other Policy Change Events Failures.
oval:mil.disa.stig.defs:def:253344	Windows must be configured to audit Other Policy Change Events Failures.
oval:mil.disa.stig.windows11:def:253345	WN11-AU-000560 - Windows 11 must be configured to audit other Logon/Logoff Events Successes.
oval:mil.disa.stig.defs:def:253345	Windows must be configured to audit other Logon/Logoff Events Successes.
oval:mil.disa.stig.windows11:def:253346	WN11-AU-000565 - Windows 11 must be configured to audit other Logon/Logoff Events Failures.
oval:mil.disa.stig.defs:def:253346	Windows must be configured to audit other Logon/Logoff Events Failures.
oval:mil.disa.stig.windows11:def:253347	WN11-AU-000570 - Windows 11 must be configured to audit Detailed File Share Failures.
oval:mil.disa.stig.defs:def:253347	Windows must be configured to audit Detailed File Share Failures.
oval:mil.disa.stig.windows11:def:253348	WN11-AU-000575 - Windows 11 must be configured to audit MPSSVC Rule-Level Policy Change Successes.

Oval ID	Title
oval:mil.disa.stig.defs:def:253348	Windows must be configured to audit MPSSVC Rule-Level Policy Change Successes.
oval:mil.disa.stig.windows11:def:253349	WN11-AU-000580 - Windows 11 must be configured to audit MPSSVC Rule-Level Policy Change Failures.
oval:mil.disa.stig.defs:def:253349	Windows must be configured to audit MPSSVC Rule-Level Policy Change Failures.
oval:mil.disa.stig.windows11:def:253352	WN11-CC-000010 - The display of slide shows on the lock screen must be disabled.
oval:mil.disa.stig.defs:def:253352	The display of slide shows on the lock screen must be disabled.
oval:mil.disa.stig.windows11:def:253353	WN11-CC-000020 - IPv6 source routing must be configured to highest protection.
oval:mil.disa.stig.defs:def:253353	IPv6 source routing must be configured to highest protection.
oval:mil.disa.stig.windows11:def:253354	WN11-CC-000025 - The system must be configured to prevent IP source routing.
oval:mil.disa.stig.defs:def:253354	The system must be configured to prevent IP source routing.
oval:mil.disa.stig.windows11:def:253355	WN11-CC-000030 - The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.
oval:mil.disa.stig.defs:def:253355	The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.
oval:mil.disa.stig.windows11:def:253356	WN11-CC-000035 - The system must be configured to ignore NetBIOS name release requests except from WINS servers.
oval:mil.disa.stig.defs:def:253356	The system must be configured to ignore NetBIOS name release requests except from WINS servers.
oval:mil.disa.stig.windows11:def:253357	WN11-CC-000037 - Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.
oval:mil.disa.stig.defs:def:253357	Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.
oval:mil.disa.stig.windows11:def:253358	WN11-CC-000038 - WDigest Authentication must be disabled.
oval:mil.disa.stig.defs:def:253358	WDigest Authentication must be disabled.
oval:mil.disa.stig.windows11:def:253359	WN11-CC-000039 - Run as different user must be removed from context menus.
oval:mil.disa.stig.defs:def:253359	Run as different user must be removed from context menus.
oval:mil.disa.stig.windows11:def:253360	WN11-CC-000040 - Insecure logons to an SMB server must be disabled.
oval:mil.disa.stig.defs:def:253360	Insecure logons to an SMB server must be disabled.
oval:mil.disa.stig.windows11:def:253361	WN11-CC-000044 - Internet connection sharing must be disabled.
oval:mil.disa.stig.defs:def:253361	Internet connection sharing must be disabled.
oval:mil.disa.stig.windows11:def:253362	WN11-CC-000050 - Hardened UNC Paths must be defined to require mutual authentication and integrity for at least the \\*\SYSVOL and \\*\NETLOGON shares.
oval:mil.disa.stig.defs:def:253362	Hardened UNC Paths must be defined to require mutual authentication and integrity for at least the \\*\SYSVOL and \\*\NETLOGON shares.
oval:mil.disa.stig.windows11:def:253364	WN11-CC-000055 - Simultaneous connections to the internet or a Windows domain must be limited.

Oval ID	Title
oval:mil.disa.stig.defs:def:253364	Simultaneous connections to the internet or a Windows domain must be limited.
oval:mil.disa.stig.windows11:def:253365	WN11-CC-000060 - Connections to non-domain networks when connected to a domain authenticated network must be blocked.
oval:mil.disa.stig.defs:def:253365	Connections to non-domain networks when connected to a domain authenticated network must be blocked.
oval:mil.disa.stig.windows11:def:253366	WN11-CC-000065 - Wi-Fi Sense must be disabled.
oval:mil.disa.stig.defs:def:253366	Wi-Fi Sense must be disabled.
oval:mil.disa.stig.windows11:def:253367	WN11-CC-000066 - Command line data must be included in process creation events.
oval:mil.disa.stig.defs:def:253367	Command line data must be included in process creation events.
oval:mil.disa.stig.windows11:def:253368	WN11-CC-000068 - Windows 11 must be configured to enable Remote host allows delegation of non-exportable credentials.
oval:mil.disa.stig.defs:def:253368	Windows must be configured to enable Remote host allows delegation of non-exportable credentials.
oval:mil.disa.stig.windows11:def:253372	WN11-CC-000085 - Early Launch Antimalware, Boot-Start Driver Initialization Policy must prevent boot drivers.
oval:mil.disa.stig.defs:def:253372	Early Launch Antimalware, Boot-Start Driver Initialization Policy must prevent boot drivers.
oval:mil.disa.stig.windows11:def:253373	WN11-CC-000090 - Group Policy objects must be reprocessed even if they have not changed.
oval:mil.disa.stig.defs:def:253373	Group Policy objects must be reprocessed even if they have not changed.
oval:mil.disa.stig.windows11:def:253374	WN11-CC-000100 - Downloading print driver packages over HTTP must be prevented.
oval:mil.disa.stig.defs:def:253374	Downloading print driver packages over HTTP must be prevented.
oval:mil.disa.stig.windows11:def:253375	WN11-CC-000105 - Web publishing and online ordering wizards must be prevented from downloading a list of providers.
oval:mil.disa.stig.defs:def:253375	Web publishing and online ordering wizards must be prevented from downloading a list of providers.
oval:mil.disa.stig.windows11:def:253376	WN11-CC-000110 - Printing over HTTP must be prevented.
oval:mil.disa.stig.defs:def:253376	Printing over HTTP must be prevented.
oval:mil.disa.stig.windows11:def:253377	WN11-CC-000115 - Systems must at least attempt device authentication using certificates.
oval:mil.disa.stig.defs:def:253377	Systems must at least attempt device authentication using certificates.
oval:mil.disa.stig.windows11:def:253378	WN11-CC-000120 - The network selection user interface (UI) must not be displayed on the logon screen.
oval:mil.disa.stig.defs:def:253378	The network selection user interface (UI) must not be displayed on the logon screen.
oval:mil.disa.stig.windows11:def:253379	WN11-CC-000130 - Local users on domain-joined computers must not be enumerated.
oval:mil.disa.stig.defs:def:253379	Local users on domain-joined computers must not be enumerated.
oval:mil.disa.stig.windows11:def:253380	WN11-CC-000145 - Users must be prompted for a password on resume from sleep (on battery).

Oval ID	Title
oval:mil.disa.stig.defs:def:253380	Users must be prompted for a password on resume from sleep (on battery).
oval:mil.disa.stig.windows11:def:253381	WN11-CC-000150 - The user must be prompted for a password on resume from sleep (plugged in).
oval:mil.disa.stig.defs:def:253381	The user must be prompted for a password on resume from sleep (plugged in).
oval:mil.disa.stig.windows11:def:253382	WN11-CC-000155 - Solicited Remote Assistance must not be allowed.
oval:mil.disa.stig.defs:def:253382	Solicited Remote Assistance must not be allowed.
oval:mil.disa.stig.windows11:def:253383	WN11-CC-000165 - Unauthenticated RPC clients must be restricted from connecting to the RPC server.
oval:mil.disa.stig.defs:def:253383	Unauthenticated RPC clients must be restricted from connecting to the RPC server.
oval:mil.disa.stig.windows11:def:253384	WN11-CC-000170 - The setting to allow Microsoft accounts to be optional for modern style apps must be enabled.
oval:mil.disa.stig.defs:def:253384	The setting to allow Microsoft accounts to be optional for modern style apps must be enabled.
oval:mil.disa.stig.windows11:def:253385	WN11-CC-000175 - The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.
oval:mil.disa.stig.defs:def:253385	The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.
oval:mil.disa.stig.windows11:def:253386	WN11-CC-000180 - Autoplay must be turned off for non-volume devices.
oval:mil.disa.stig.defs:def:253386	Autoplay must be turned off for non-volume devices.
oval:mil.disa.stig.windows11:def:253387	WN11-CC-000185 - The default autorun behavior must be configured to prevent autorun commands.
oval:mil.disa.stig.defs:def:253387	The default autorun behavior must be configured to prevent autorun commands.
oval:mil.disa.stig.windows11:def:253388	WN11-CC-000190 - Autoplay must be disabled for all drives.
oval:mil.disa.stig.defs:def:253388	Autoplay must be disabled for all drives.
oval:mil.disa.stig.windows11:def:253389	WN11-CC-000195 - Enhanced anti-spoofing for facial recognition must be enabled on Windows 11.
oval:mil.disa.stig.defs:def:253389	Enhanced anti-spoofing for facial recognition must be enabled on Windows.
oval:mil.disa.stig.windows11:def:253390	WN11-CC-000197 - Microsoft consumer experiences must be turned off.
oval:mil.disa.stig.defs:def:253390	Microsoft consumer experiences must be turned off.
oval:mil.disa.stig.windows11:def:253391	WN11-CC-000200 - Administrator accounts must not be enumerated during elevation.
oval:mil.disa.stig.defs:def:253391	Administrator accounts must not be enumerated during elevation.
oval:mil.disa.stig.windows11:def:253393	WN11-CC-000205 - Windows Telemetry must not be configured to Full.
oval:mil.disa.stig.defs:def:253393	Windows Telemetry must not be configured to Full.
oval:mil.disa.stig.windows11:def:253394	WN11-CC-000206 - Windows Update must not obtain updates from other PCs on the internet.
oval:mil.disa.stig.defs:def:253394	Windows Update for workstations must not obtain updates from other PCs on the internet.
oval:mil.disa.stig.defs:def:254357	Windows Update must not obtain updates from other PCs on the internet.

Oval ID	Title
oval:mil.disa.stig.windows11:def:253395	WN11-CC-000210 - The Microsoft Defender SmartScreen for Explorer must be enabled.
oval:mil.disa.stig.defs:def:253395	The Microsoft Defender SmartScreen for Explorer must be enabled.
oval:mil.disa.stig.windows11:def:253396	WN11-CC-000215 - Explorer Data Execution Prevention must be enabled.
oval:mil.disa.stig.defs:def:253396	Explorer Data Execution Prevention must be enabled.
oval:mil.disa.stig.windows11:def:253397	WN11-CC-000220 - File Explorer heap termination on corruption must be disabled.
oval:mil.disa.stig.defs:def:253397	File Explorer heap termination on corruption must be disabled.
oval:mil.disa.stig.windows11:def:253398	WN11-CC-000225 - File Explorer shell protocol must run in protected mode.
oval:mil.disa.stig.defs:def:253398	File Explorer shell protocol must run in protected mode.
oval:mil.disa.stig.windows11:def:253399	WN11-CC-000252 - Windows 11 must be configured to disable Windows Game Recording and Broadcasting.
oval:mil.disa.stig.defs:def:253399	Windows must be configured to disable Windows Game Recording and Broadcasting.
oval:mil.disa.stig.windows11:def:253400	WN11-CC-000255 - The use of a hardware security device with Windows Hello for Business must be enabled.
oval:mil.disa.stig.defs:def:253400	The use of a hardware security device with Windows Hello for Business must be enabled.
oval:mil.disa.stig.windows11:def:253401	WN11-CC-000260 - Windows 11 must be configured to require a minimum pin length of six characters or greater.
oval:mil.disa.stig.defs:def:253401	Windows must be configured to require a minimum pin length of six characters or greater.
oval:mil.disa.stig.windows11:def:253402	WN11-CC-000270 - Passwords must not be saved in the Remote Desktop Client.
oval:mil.disa.stig.defs:def:253402	Passwords must not be saved in the Remote Desktop Client.
oval:mil.disa.stig.windows11:def:253403	WN11-CC-000275 - Local drives must be prevented from sharing with Remote Desktop Session Hosts.
oval:mil.disa.stig.defs:def:253403	Local drives must be prevented from sharing with Remote Desktop Session Hosts.
oval:mil.disa.stig.windows11:def:253404	WN11-CC-000280 - Remote Desktop Services must always prompt a client for passwords upon connection.
oval:mil.disa.stig.defs:def:253404	Remote Desktop Services must always prompt a client for passwords upon connection.
oval:mil.disa.stig.windows11:def:253405	WN11-CC-000285 - The Remote Desktop Session Host must require secure RPC communications.
oval:mil.disa.stig.defs:def:253405	The Remote Desktop Session Host must require secure RPC communications.
oval:mil.disa.stig.windows11:def:253406	WN11-CC-000290 - Remote Desktop Services must be configured with the client connection encryption set to the required level.
oval:mil.disa.stig.defs:def:253406	Remote Desktop Services must be configured with the client connection encryption set to the required level.
oval:mil.disa.stig.windows11:def:253407	WN11-CC-000295 - Attachments must be prevented from being downloaded from RSS feeds.
oval:mil.disa.stig.defs:def:253407	Attachments must be prevented from being downloaded from RSS feeds.

Oval ID	Title
oval:mil.disa.stig.windows11:def:253408	WN11-CC-000300 - Basic authentication for RSS feeds over HTTP must not be used.
oval:mil.disa.stig.defs:def:253408	Basic authentication for RSS feeds over HTTP must not be used.
oval:mil.disa.stig.windows11:def:253409	WN11-CC-000305 - Indexing of encrypted files must be turned off.
oval:mil.disa.stig.defs:def:253409	Indexing of encrypted files must be turned off.
oval:mil.disa.stig.windows11:def:253410	WN11-CC-000310 - Users must be prevented from changing installation options.
oval:mil.disa.stig.defs:def:253410	Users must be prevented from changing installation options.
oval:mil.disa.stig.windows11:def:253411	WN11-CC-000315 - The Windows Installer feature "Always install with elevated privileges" must be disabled.
oval:mil.disa.stig.defs:def:253411	The Windows Installer feature "Always install with elevated privileges" must be disabled.
oval:mil.disa.stig.windows11:def:253412	WN11-CC-000320 - Users must be notified if a web-based program attempts to install software.
oval:mil.disa.stig.defs:def:253412	Users must be notified if a web-based program attempts to install software.
oval:mil.disa.stig.windows11:def:253413	WN11-CC-000325 - Automatically signing in the last interactive user after a system-initiated restart must be disabled.
oval:mil.disa.stig.defs:def:253413	Automatically signing in the last interactive user after a system-initiated restart must be disabled.
oval:mil.disa.stig.windows11:def:253414	WN11-CC-000326 - PowerShell script block logging must be enabled on Windows 11.
oval:mil.disa.stig.defs:def:253414	PowerShell script block logging must be enabled on Windows.
oval:mil.disa.stig.windows11:def:253415	WN11-CC-000327 - PowerShell Transcription must be enabled on Windows 11.
oval:mil.disa.stig.defs:def:253415	PowerShell Transcription must be enabled on Windows.
oval:mil.disa.stig.windows11:def:253416	WN11-CC-000330 - The Windows Remote Management (WinRM) client must not use Basic authentication.
oval:mil.disa.stig.defs:def:253416	The Windows Remote Management (WinRM) client must not use Basic authentication.
oval:mil.disa.stig.windows11:def:253417	WN11-CC-000335 - The Windows Remote Management (WinRM) client must not allow unencrypted traffic.
oval:mil.disa.stig.defs:def:253417	The Windows Remote Management (WinRM) client must not allow unencrypted traffic.
oval:mil.disa.stig.windows11:def:253418	WN11-CC-000345 - The Windows Remote Management (WinRM) service must not use Basic authentication.
oval:mil.disa.stig.defs:def:253418	The Windows Remote Management (WinRM) service must not use Basic authentication.
oval:mil.disa.stig.windows11:def:253419	WN11-CC-000350 - The Windows Remote Management (WinRM) service must not allow unencrypted traffic.
oval:mil.disa.stig.defs:def:254382	The Windows Remote Management (WinRM) service must not allow unencrypted traffic.
oval:mil.disa.stig.windows11:def:253420	WN11-CC-000355 - The Windows Remote Management (WinRM) service must not store RunAs credentials.

Oval ID	Title
oval:mil.disa.stig.defs:def:253420	The Windows Remote Management (WinRM) service must not store RunAs credentials.
oval:mil.disa.stig.windows11:def:253421	WN11-CC-000360 - The Windows Remote Management (WinRM) client must not use Digest authentication.
oval:mil.disa.stig.defs:def:253421	The Windows Remote Management (WinRM) client must not use Digest authentication.
oval:mil.disa.stig.windows11:def:253422	WN11-CC-000365 - Windows 11 must be configured to prevent Windows apps from being activated by voice while the system is locked.
oval:mil.disa.stig.defs:def:253422	Windows must be configured to prevent Windows apps from being activated by voice while the system is locked.
oval:mil.disa.stig.windows11:def:253423	WN11-CC-000370 - The convenience PIN for Windows 11 must be disabled.
oval:mil.disa.stig.defs:def:253423	The convenience PIN for Windows must be disabled.
oval:mil.disa.stig.windows11:def:253424	WN11-CC-000385 - Windows Ink Workspace must be configured to disallow access above the lock.
oval:mil.disa.stig.defs:def:253424	Windows Ink Workspace must be configured to disallow access above the lock.
oval:mil.disa.stig.windows11:def:253426	WN11-EP-000310 - Windows 11 Kernel (Direct Memory Access) DMA Protection must be enabled.
oval:mil.disa.stig.defs:def:253426	Windows Kernel (Direct Memory Access) DMA Protection must be enabled.
oval:mil.disa.stig.windows11:def:253427	WN11-PK-000005 - The DoD Root CA certificates must be installed in the Trusted Root Store.
oval:mil.disa.stig.defs:def:253427	The DoD Root CA certificates must be installed in the Trusted Root Store.
oval:mil.disa.stig.windows11:def:253428	WN11-PK-000010 - The External Root CA certificates must be installed in the Trusted Root Store on unclassified systems.
oval:mil.disa.stig.defs:def:253428	The External Root CA certificates must be installed in the Trusted Root Store on unclassified systems.
oval:mil.disa.stig.windows11:def:253429	WN11-PK-000015 - The DoD Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.
oval:mil.disa.stig.defs:def:253429	The DoD Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.
oval:mil.disa.stig.windows11:def:253430	WN11-PK-000020 - The US DoD CCEB Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.
oval:mil.disa.stig.defs:def:253430	The US DoD CCEB Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.
oval:mil.disa.stig.windows11:def:253432	WN11-SO-000005 - The built-in administrator account must be disabled.
oval:mil.disa.stig.defs:def:253432	The built-in administrator account must be disabled.
oval:mil.disa.stig.windows11:def:253433	WN11-SO-000010 - The built-in guest account must be disabled.
oval:mil.disa.stig.defs:def:253433	The built-in guest account must be disabled.
oval:mil.disa.stig.windows11:def:253434	WN11-SO-000015 - Local accounts with blank passwords must be restricted to prevent access from the network.
oval:mil.disa.stig.defs:def:253434	Local accounts with blank passwords must be restricted to prevent access from the network.
oval:mil.disa.stig.windows11:def:253435	WN11-SO-000020 - The built-in administrator account must be renamed.

Oval ID	Title
oval:mil.disa.stig.defs:def:253435	The built-in administrator account must be renamed.
oval:mil.disa.stig.windows11:def:253436	WN11-SO-000025 - The built-in guest account must be renamed.
oval:mil.disa.stig.defs:def:253436	The built-in guest account must be renamed.
oval:mil.disa.stig.windows11:def:253437	WN11-SO-000030 - Audit policy using subcategories must be enabled.
oval:mil.disa.stig.defs:def:253437	Audit policy using subcategories must be enabled.
oval:mil.disa.stig.windows11:def:253438	WN11-SO-000035 - Outgoing secure channel traffic must be encrypted or signed.
oval:mil.disa.stig.defs:def:253438	Outgoing secure channel traffic must be encrypted or signed.
oval:mil.disa.stig.windows11:def:253439	WN11-SO-000040 - Outgoing secure channel traffic must be encrypted.
oval:mil.disa.stig.defs:def:253439	Outgoing secure channel traffic must be encrypted.
oval:mil.disa.stig.windows11:def:253440	WN11-SO-000045 - Outgoing secure channel traffic must be signed.
oval:mil.disa.stig.defs:def:253440	Outgoing secure channel traffic must be signed.
oval:mil.disa.stig.windows11:def:253441	WN11-SO-000050 - The computer account password must not be prevented from being reset.
oval:mil.disa.stig.defs:def:253441	The computer account password must not be prevented from being reset.
oval:mil.disa.stig.windows11:def:253442	WN11-SO-000055 - The maximum age for machine account passwords must be configured to 30 days or less.
oval:mil.disa.stig.defs:def:253442	The maximum age for machine account passwords must be configured to 30 days or less.
oval:mil.disa.stig.windows11:def:253443	WN11-SO-000060 - The system must be configured to require a strong session key.
oval:mil.disa.stig.defs:def:253443	The system must be configured to require a strong session key.
oval:mil.disa.stig.windows11:def:253444	WN11-SO-000070 - The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.
oval:mil.disa.stig.defs:def:253444	The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.
oval:mil.disa.stig.windows11:def:253447	WN11-SO-000085 - Caching of logon credentials must be limited.
oval:mil.disa.stig.defs:def:253447	Caching of logon credentials must be limited.
oval:mil.disa.stig.windows11:def:253448	WN11-SO-000095 - The Smart Card removal option must be configured to Force Logoff or Lock Workstation.
oval:mil.disa.stig.defs:def:253448	The Smart Card removal option must be configured to Force Logoff or Lock Workstation.
oval:mil.disa.stig.windows11:def:253449	WN11-SO-000100 - The Windows SMB client must be configured to always perform SMB packet signing.
oval:mil.disa.stig.defs:def:253449	The Windows SMB client must be configured to always perform SMB packet signing.
oval:mil.disa.stig.windows11:def:253450	WN11-SO-000110 - Unencrypted passwords must not be sent to third-party SMB Servers.
oval:mil.disa.stig.defs:def:253450	Unencrypted passwords must not be sent to third-party SMB Servers.
oval:mil.disa.stig.windows11:def:253451	WN11-SO-000120 - The Windows SMB server must be configured to always perform SMB packet signing.

Oval ID	Title
oval:mil.disa.stig.defs:def:253451	The Windows SMB server must be configured to always perform SMB packet signing.
oval:mil.disa.stig.windows11:def:253453	WN11-SO-000145 - Anonymous enumeration of SAM accounts must not be allowed.
oval:mil.disa.stig.defs:def:253453	Anonymous enumeration of SAM accounts must not be allowed.
oval:mil.disa.stig.windows11:def:253454	WN11-SO-000150 - Anonymous enumeration of shares must be restricted.
oval:mil.disa.stig.defs:def:253454	Anonymous enumeration of shares must be restricted.
oval:mil.disa.stig.windows11:def:253455	WN11-SO-000160 - The system must be configured to prevent anonymous users from having the same rights as the Everyone group.
oval:mil.disa.stig.defs:def:253455	The system must be configured to prevent anonymous users from having the same rights as the Everyone group.
oval:mil.disa.stig.windows11:def:253456	WN11-SO-000165 - Anonymous access to Named Pipes and Shares must be restricted.
oval:mil.disa.stig.defs:def:253456	Anonymous access to Named Pipes and Shares must be restricted.
oval:mil.disa.stig.windows11:def:253457	WN11-SO-000167 - Remote calls to the Security Account Manager (SAM) must be restricted to Administrators.
oval:mil.disa.stig.defs:def:253457	Remote calls to the Security Account Manager (SAM) must be restricted to Administrators.
oval:mil.disa.stig.windows11:def:253458	WN11-SO-000180 - NTLM must be prevented from falling back to a Null session.
oval:mil.disa.stig.defs:def:253458	NTLM must be prevented from falling back to a Null session.
oval:mil.disa.stig.windows11:def:253459	WN11-SO-000185 - PKU2U authentication using online identities must be prevented.
oval:mil.disa.stig.defs:def:253459	PKU2U authentication using online identities must be prevented.
oval:mil.disa.stig.windows11:def:253460	WN11-SO-000190 - Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.
oval:mil.disa.stig.defs:def:253460	Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.
oval:mil.disa.stig.windows11:def:253461	WN11-SO-000195 - The system must be configured to prevent the storage of the LAN Manager hash of passwords.
oval:mil.disa.stig.defs:def:253461	The system must be configured to prevent the storage of the LAN Manager hash of passwords.
oval:mil.disa.stig.windows11:def:253462	WN11-SO-000205 - The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.
oval:mil.disa.stig.defs:def:253462	The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.
oval:mil.disa.stig.windows11:def:253463	WN11-SO-000210 - The system must be configured to the required LDAP client signing level.
oval:mil.disa.stig.defs:def:253463	The system must be configured to the required LDAP client signing level.
oval:mil.disa.stig.windows11:def:253464	WN11-SO-000215 - The system must be configured to meet the minimum session security requirement for NTLM SSP based clients.
oval:mil.disa.stig.defs:def:253464	The system must be configured to meet the minimum session security requirement for NTLM SSP based clients.

Oval ID	Title
oval:mil.disa.stig.windows11:def:253465	WN11-SO-000220 - The system must be configured to meet the minimum session security requirement for NTLM SSP based servers.
oval:mil.disa.stig.defs:def:253465	The system must be configured to meet the minimum session security requirement for NTLM SSP based servers.
oval:mil.disa.stig.windows11:def:253466	WN11-SO-000230 - The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.
oval:mil.disa.stig.defs:def:253466	The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.
oval:mil.disa.stig.windows11:def:253467	WN11-SO-000240 - The default permissions of global system objects must be increased.
oval:mil.disa.stig.defs:def:253467	The default permissions of global system objects must be increased.
oval:mil.disa.stig.windows11:def:253468	WN11-SO-000245 - User Account Control approval mode for the built-in Administrator must be enabled.
oval:mil.disa.stig.defs:def:253468	User Account Control approval mode for the built-in Administrator must be enabled.
oval:mil.disa.stig.windows11:def:253469	WN11-SO-000250 - User Account Control must prompt administrators for consent on the secure desktop.
oval:mil.disa.stig.defs:def:253469	User Account Control must prompt administrators for consent on the secure desktop.
oval:mil.disa.stig.windows11:def:253470	WN11-SO-000251 - Windows 11 must use multifactor authentication for local and network access to privileged and non-privileged accounts.
oval:mil.disa.stig.defs:def:253470	Windows must use multifactor authentication for local and network access to privileged and non-privileged accounts.
oval:mil.disa.stig.windows11:def:253471	WN11-SO-000255 - User Account Control must automatically deny elevation requests for standard users.
oval:mil.disa.stig.defs:def:253471	User Account Control must automatically deny elevation requests for standard users.
oval:mil.disa.stig.windows11:def:253472	WN11-SO-000260 - User Account Control must be configured to detect application installations and prompt for elevation.
oval:mil.disa.stig.defs:def:253472	User Account Control must be configured to detect application installations and prompt for elevation.
oval:mil.disa.stig.windows11:def:253473	WN11-SO-000265 - User Account Control must only elevate UIAccess applications that are installed in secure locations.
oval:mil.disa.stig.defs:def:253473	User Account Control must only elevate UIAccess applications that are installed in secure locations.
oval:mil.disa.stig.windows11:def:253474	WN11-SO-000270 - User Account Control must run all administrators in Admin Approval Mode, enabling UAC.
oval:mil.disa.stig.defs:def:253474	User Account Control must run all administrators in Admin Approval Mode, enabling UAC.
oval:mil.disa.stig.windows11:def:253475	WN11-SO-000275 - User Account Control must virtualize file and registry write failures to per-user locations.
oval:mil.disa.stig.defs:def:253475	User Account Control must virtualize file and registry write failures to per-user locations.
oval:mil.disa.stig.windows11:def:253479	WN11-UR-000005 - The "Access Credential Manager as a trusted caller" user right must not be assigned to any groups or accounts.

Oval ID	Title
oval:mil.disa.stig.defs:def:253479	The "Access Credential Manager as a trusted caller" user right must not be assigned to any groups or accounts.
oval:mil.disa.stig.windows11:def:253480	WN11-UR-000010 - The "Access this computer from the network" user right must only be assigned to the Administrators and Remote Desktop Users groups.
oval:mil.disa.stig.defs:def:253480	The "Access this computer from the network" user right must only be assigned to the Administrators and Remote Desktop Users groups.
oval:mil.disa.stig.windows11:def:253481	WN11-UR-000015 - The "Act as part of the operating system" user right must not be assigned to any groups or accounts.
oval:mil.disa.stig.defs:def:253481	The "Act as part of the operating system" user right must not be assigned to any groups or accounts.
oval:mil.disa.stig.windows11:def:253482	WN11-UR-000025 - The "Allow log on locally" user right must only be assigned to the Administrators and Users groups.
oval:mil.disa.stig.defs:def:253482	The "Allow log on locally" user right must only be assigned to the Administrators and Users groups.
oval:mil.disa.stig.windows11:def:253483	WN11-UR-000030 - The "Back up files and directories" user right must only be assigned to the Administrators group.
oval:mil.disa.stig.defs:def:253483	The "Back up files and directories" user right must only be assigned to the Administrators group.
oval:mil.disa.stig.windows11:def:253484	WN11-UR-000035 - The "Change the system time" user right must only be assigned to Administrators and Local Service.
oval:mil.disa.stig.defs:def:253484	The "Change the system time" user right must only be assigned to Administrators and Local Service.
oval:mil.disa.stig.windows11:def:253485	WN11-UR-000040 - The "Create a pagefile" user right must only be assigned to the Administrators group.
oval:mil.disa.stig.defs:def:253485	The "Create a pagefile" user right must only be assigned to the Administrators group.
oval:mil.disa.stig.windows11:def:253486	WN11-UR-000045 - The "Create a token object" user right must not be assigned to any groups or accounts.
oval:mil.disa.stig.defs:def:253486	The "Create a token object" user right must not be assigned to any groups or accounts.
oval:mil.disa.stig.windows11:def:253487	WN11-UR-000050 - The "Create global objects" user right must only be assigned to Administrators, Service, Local Service, and Network Service.
oval:mil.disa.stig.defs:def:253487	The "Create global objects" user right must only be assigned to Administrators, Service, Local Service, and Network Service.
oval:mil.disa.stig.windows11:def:253488	WN11-UR-000055 - The "Create permanent shared objects" user right must not be assigned to any groups or accounts.
oval:mil.disa.stig.defs:def:253488	The "Create permanent shared objects" user right must not be assigned to any groups or accounts.
oval:mil.disa.stig.windows11:def:253489	WN11-UR-000060 - The "Create symbolic links" user right must only be assigned to the Administrators group.
oval:mil.disa.stig.defs:def:253489	The "Create symbolic links" user right must only be assigned to the Administrators group.
oval:mil.disa.stig.windows11:def:253490	WN11-UR-000065 - The "Debug programs" user right must only be assigned to the Administrators group.

Oval ID	Title
oval:mil.disa.stig.defs:def:253490	The "Debug programs" user right must only be assigned to the Administrators group.
oval:mil.disa.stig.windows11:def:253491	WN11-UR-000070 - The "Deny access to this computer from the network" user right on workstations must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems and unauthenticated access on all systems.
oval:mil.disa.stig.defs:def:253491	The "Deny access to this computer from the network" user right on workstations must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems and unauthenticated access on all systems.
oval:mil.disa.stig.windows11:def:253492	WN11-UR-000075 - The "Deny log on as a batch job" user right on domain-joined workstations must be configured to prevent access from highly privileged domain accounts.
oval:mil.disa.stig.defs:def:253492	The "Deny log on as a batch job" user right on domain-joined workstations must be configured to prevent access from highly privileged domain accounts.
oval:mil.disa.stig.windows11:def:253493	WN11-UR-000080 - The "Deny log on as a service" user right on Windows 11 domain-joined workstations must be configured to prevent access from highly privileged domain accounts.
oval:mil.disa.stig.defs:def:253493	The "Deny log on as a service" user right on Windows domain-joined workstations must be configured to prevent access from highly privileged domain accounts.
oval:mil.disa.stig.windows11:def:253494	WN11-UR-000085 - The "Deny log on locally" user right on workstations must be configured to prevent access from highly privileged domain accounts on domain systems and unauthenticated access on all systems.
oval:mil.disa.stig.defs:def:253494	The "Deny log on locally" user right on workstations must be configured to prevent access from highly privileged domain accounts on domain systems and unauthenticated access on all systems.
oval:mil.disa.stig.windows11:def:253495	WN11-UR-000090 - The "Deny log on through Remote Desktop Services" user right on Windows 11 workstations must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems and unauthenticated access on all systems.
oval:mil.disa.stig.defs:def:253495	The "Deny log on through Remote Desktop Services" user right on Windows workstations must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems and unauthenticated access on all systems.
oval:mil.disa.stig.windows11:def:253496	WN11-UR-000095 - The "Enable computer and user accounts to be trusted for delegation" user right must not be assigned to any groups or accounts.
oval:mil.disa.stig.defs:def:253496	The "Enable computer and user accounts to be trusted for delegation" user right must not be assigned to any groups or accounts.
oval:mil.disa.stig.windows11:def:253497	WN11-UR-000100 - The "Force shutdown from a remote system" user right must only be assigned to the Administrators group.
oval:mil.disa.stig.defs:def:253497	The "Force shutdown from a remote system" user right must only be assigned to the Administrators group.
oval:mil.disa.stig.windows11:def:253498	WN11-UR-000110 - The "Impersonate a client after authentication" user right must only be assigned to Administrators, Service, Local Service, and Network Service.
oval:mil.disa.stig.defs:def:253498	The "Impersonate a client after authentication" user right must only be assigned to Administrators, Service, Local Service, and Network Service.
oval:mil.disa.stig.windows11:def:253499	WN11-UR-000120 - The "Load and unload device drivers" user right must only be assigned to the Administrators group.

Oval ID	Title
oval:mil.disa.stig.defs:def:253499	The "Load and unload device drivers" user right must only be assigned to the Administrators group.
oval:mil.disa.stig.windows11:def:253500	WN11-UR-000125 - The "Lock pages in memory" user right must not be assigned to any groups or accounts.
oval:mil.disa.stig.defs:def:253500	The "Lock pages in memory" user right must not be assigned to any groups or accounts.
oval:mil.disa.stig.windows11:def:253501	WN11-UR-000130 - The "Manage auditing and security log" user right must only be assigned to the Administrators group.
oval:mil.disa.stig.defs:def:253501	The "Manage auditing and security log" user right must only be assigned to the Administrators group.
oval:mil.disa.stig.windows11:def:253502	WN11-UR-000140 - The "Modify firmware environment values" user right must only be assigned to the Administrators group.
oval:mil.disa.stig.defs:def:253502	The "Modify firmware environment values" user right must only be assigned to the Administrators group.
oval:mil.disa.stig.windows11:def:253503	WN11-UR-000145 - The "Perform volume maintenance tasks" user right must only be assigned to the Administrators group.
oval:mil.disa.stig.defs:def:253503	The "Perform volume maintenance tasks" user right must only be assigned to the Administrators group.
oval:mil.disa.stig.windows11:def:253504	WN11-UR-000150 - The "Profile single process" user right must only be assigned to the Administrators group.
oval:mil.disa.stig.defs:def:253504	The "Profile single process" user right must only be assigned to the Administrators group.
oval:mil.disa.stig.windows11:def:253505	WN11-UR-000160 - The "Restore files and directories" user right must only be assigned to the Administrators group.
oval:mil.disa.stig.defs:def:253505	The "Restore files and directories" user right must only be assigned to the Administrators group.
oval:mil.disa.stig.windows11:def:253506	WN11-UR-000165 - The "Take ownership of files or other objects" user right must only be assigned to the Administrators group.
oval:mil.disa.stig.defs:def:253506	The "Take ownership of files or other objects" user right must only be assigned to the Administrators group.
oval:mil.disa.stig.windows:def:220812	WN10-CC-000075 - Credential Guard must be running on Windows 10 domain-joined systems.
oval:mil.disa.stig.windows2022:def:254247	WN22-00-000100 - Windows Server 2022 must be maintained at a supported servicing level.
oval:mil.disa.stig.defs:def:254247	Windows must be maintained at a supported servicing level.
oval:mil.disa.stig.windows2022:def:254250	WN22-00-000130 - Windows Server 2022 local volumes must use a format that supports NTFS attributes.
oval:mil.disa.stig.defs:def:254250	Windows local volumes must use a format that supports NTFS attributes.
oval:mil.disa.stig.windows2022:def:254269	WN22-00-000320 - Windows Server 2022 must not have the Fax Server role installed.
oval:mil.disa.stig.defs:def:254269	Windows must not have the Fax Server role installed.
oval:mil.disa.stig.windows2022:def:254270	WN22-00-000330 - Windows Server 2022 must not have the Microsoft FTP service installed unless required by the organization.

Oval ID	Title
oval:mil.disa.stig.defs:def:254270	Windows must not have the Microsoft FTP service installed unless required by the organization.
oval:mil.disa.stig.windows2022:def:254271	WN22-00-000340 - Windows Server 2022 must not have the Peer Name Resolution Protocol installed.
oval:mil.disa.stig.defs:def:254271	Windows must not have the Peer Name Resolution Protocol installed.
oval:mil.disa.stig.windows2022:def:254272	WN22-00-000350 - Windows Server 2022 must not have Simple TCP/IP Services installed.
oval:mil.disa.stig.windows2022:def:254273	WN22-00-000360 - Windows Server 2022 must not have the Telnet Client installed.
oval:mil.disa.stig.windows2022:def:254274	WN22-00-000370 - Windows Server 2022 must not have the TFTP Client installed.
oval:mil.disa.stig.windows2022:def:254275	WN22-00-000380 - Windows Server 2022 must not the Server Message Block (SMB) v1 protocol installed.
oval:mil.disa.stig.windows2022:def:254276	WN22-00-000390 - Windows Server 2022 must have the Server Message Block (SMB) v1 protocol disabled on the SMB server.
oval:mil.disa.stig.windows2022:def:254277	WN22-00-000400 - Windows Server 2022 must have the Server Message Block (SMB) v1 protocol disabled on the SMB client.
oval:mil.disa.stig.windows2022:def:254278	WN22-00-000410 - Windows Server 2022 must not have Windows PowerShell 2.0 installed.
oval:mil.disa.stig.defs:def:254278	The Windows PowerShell 2.0 feature must be disabled on the system.
oval:mil.disa.stig.windows2022:def:254285	WN22-AC-000010 - Windows Server 2022 account lockout duration must be configured to 15 minutes or greater.
oval:mil.disa.stig.windows2022:def:254286	WN22-AC-000020 - Windows Server 2022 must have the number of allowed bad logon attempts configured to three or less.
oval:mil.disa.stig.windows2022:def:254287	WN22-AC-000030 - Windows Server 2022 must have the period of time before the bad logon counter is reset configured to 15 minutes or greater.
oval:mil.disa.stig.windows2022:def:254288	WN22-AC-000040 - Windows Server 2022 password history must be configured to 24 passwords remembered.
oval:mil.disa.stig.windows2022:def:254289	WN22-AC-000050 - Windows Server 2022 maximum password age must be configured to 60 days or less.
oval:mil.disa.stig.windows2022:def:254290	WN22-AC-000060 - Windows Server 2022 minimum password age must be configured to at least one day.
oval:mil.disa.stig.windows2022:def:254291	WN22-AC-000070 - Windows Server 2022 minimum password length must be configured to 14 characters.
oval:mil.disa.stig.windows2022:def:254292	WN22-AC-000080 - Windows Server 2022 must have the built-in Windows password complexity policy enabled.
oval:mil.disa.stig.windows2022:def:254293	WN22-AC-000090 - Windows Server 2022 reversible password encryption must be disabled.
oval:mil.disa.stig.windows2022:def:254296	WN22-AU-000030 - Windows Server 2022 permissions for the Application event log must prevent access by nonprivileged accounts.
oval:mil.disa.stig.defs:def:254296	Windows permissions for the Application event log must prevent access by non-privileged accounts.
oval:mil.disa.stig.windows2022:def:254297	WN22-AU-000040 - Windows Server 2022 permissions for the Security event log must prevent access by nonprivileged accounts.

Oval ID	Title
oval:mil.disa.stig.defs:def:254297	Windows permissions for the Security event log must prevent access by non-privileged accounts.
oval:mil.disa.stig.windows2022:def:254298	WN22-AU-000050 - Windows Server 2022 permissions for the System event log must prevent access by nonprivileged accounts.
oval:mil.disa.stig.defs:def:254298	Windows permissions for the System event log must prevent access by non-privileged accounts.
oval:mil.disa.stig.windows2022:def:254299	WN22-AU-000060 - Windows Server 2022 Event Viewer must be protected from unauthorized modification and deletion.
oval:mil.disa.stig.defs:def:254299	Windows Event Viewer must be protected from unauthorized modification and deletion.
oval:mil.disa.stig.windows2022:def:254300	WN22-AU-000070 - Windows Server 2022 must be configured to audit Account Logon - Credential Validation successes.
oval:mil.disa.stig.windows2022:def:254301	WN22-AU-000080 - Windows Server 2022 must be configured to audit Account Logon - Credential Validation failures.
oval:mil.disa.stig.windows2022:def:254302	WN22-AU-000090 - Windows Server 2022 must be configured to audit Account Management - Other Account Management Events successes.
oval:mil.disa.stig.defs:def:254302	Windows must be configured to audit Account Management - Other Account Management Events successes.
oval:mil.disa.stig.windows2022:def:254303	WN22-AU-000100 - Windows Server 2022 must be configured to audit Account Management - Security Group Management successes.
oval:mil.disa.stig.windows2022:def:254304	WN22-AU-000110 - Windows Server 2022 must be configured to audit Account Management - User Account Management successes.
oval:mil.disa.stig.windows2022:def:254305	WN22-AU-000120 - Windows Server 2022 must be configured to audit Account Management - User Account Management failures.
oval:mil.disa.stig.windows2022:def:254307	WN22-AU-000140 - Windows Server 2022 must be configured to audit Detailed Tracking - Process Creation successes.
oval:mil.disa.stig.windows2022:def:254309	WN22-AU-000160 - Windows Server 2022 must be configured to audit Logon/Logoff - Account Lockout failures.
oval:mil.disa.stig.windows2022:def:254311	WN22-AU-000180 - Windows Server 2022 must be configured to audit logoff successes.
oval:mil.disa.stig.windows2022:def:254312	WN22-AU-000190 - Windows Server 2022 must be configured to audit logon successes.
oval:mil.disa.stig.windows2022:def:254313	WN22-AU-000200 - Windows Server 2022 must be configured to audit logon failures.
oval:mil.disa.stig.windows2022:def:254314	WN22-AU-000210 - Windows Server 2022 must be configured to audit Logon/Logoff - Special Logon successes.
oval:mil.disa.stig.windows2022:def:254315	WN22-AU-000220 - Windows Server 2022 must be configured to audit Object Access - Other Object Access Events successes.
oval:mil.disa.stig.windows2022:def:254316	WN22-AU-000230 - Windows Server 2022 must be configured to audit Object Access - Other Object Access Events failures.
oval:mil.disa.stig.windows2022:def:254319	WN22-AU-000260 - Windows Server 2022 must be configured to audit Policy Change - Audit Policy Change successes.
oval:mil.disa.stig.windows2022:def:254320	WN22-AU-000270 - Windows Server 2022 must be configured to audit Policy Change - Audit Policy Change failures.
oval:mil.disa.stig.defs:def:254320	Windows must be configured to audit Policy Change - Audit Policy Change failures.

Oval ID	Title
oval:mil.disa.stig.windows2022:def:254321	WN22-AU-000280 - Windows Server 2022 must be configured to audit Policy Change - Authentication Policy Change successes.
oval:mil.disa.stig.windows2022:def:254322	WN22-AU-000290 - Windows Server 2022 must be configured to audit Policy Change - Authorization Policy Change successes.
oval:mil.disa.stig.windows2022:def:254323	WN22-AU-000300 - Windows Server 2022 must be configured to audit Privilege Use - Sensitive Privilege Use successes.
oval:mil.disa.stig.windows2022:def:254324	WN22-AU-000310 - Windows Server 2022 must be configured to audit Privilege Use - Sensitive Privilege Use failures.
oval:mil.disa.stig.windows2022:def:254325	WN22-AU-000320 - Windows Server 2022 must be configured to audit System - IPsec Driver successes.
oval:mil.disa.stig.defs:def:254325	Windows must be configured to audit System - IPsec Driver successes.
oval:mil.disa.stig.windows2022:def:254326	WN22-AU-000330 - Windows Server 2022 must be configured to audit System - IPsec Driver failures.
oval:mil.disa.stig.windows2022:def:254327	WN22-AU-000340 - Windows Server 2022 must be configured to audit System - Other System Events successes.
oval:mil.disa.stig.windows2022:def:254328	WN22-AU-000350 - Windows Server 2022 must be configured to audit System - Other System Events failures.
oval:mil.disa.stig.windows2022:def:254329	WN22-AU-000360 - Windows Server 2022 must be configured to audit System - Security State Change successes.
oval:mil.disa.stig.windows2022:def:254330	WN22-AU-000370 - Windows Server 2022 must be configured to audit System - Security System Extension successes.
oval:mil.disa.stig.windows2022:def:254331	WN22-AU-000380 - Windows Server 2022 must be configured to audit System - System Integrity successes.
oval:mil.disa.stig.windows2022:def:254332	WN22-AU-000390 - Windows Server 2022 must be configured to audit System - System Integrity failures.
oval:mil.disa.stig.windows2022:def:254333	WN22-CC-000010 - Windows Server 2022 must prevent the display of slide shows on the lock screen.
oval:mil.disa.stig.windows2022:def:254334	WN22-CC-000020 - Windows Server 2022 must have WDigest Authentication disabled.
oval:mil.disa.stig.windows2022:def:254335	WN22-CC-000030 - Windows Server 2022 Internet Protocol version 6 (IPv6) source routing must be configured to the highest protection level to prevent IP source routing.
oval:mil.disa.stig.windows2022:def:254336	WN22-CC-000040 - Windows Server 2022 source routing must be configured to the highest protection level to prevent Internet Protocol (IP) source routing.
oval:mil.disa.stig.windows2022:def:254337	WN22-CC-000050 - Windows Server 2022 must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF)-generated routes.
oval:mil.disa.stig.windows2022:def:254338	WN22-CC-000060 - Windows Server 2022 must be configured to ignore NetBIOS name release requests except from WINS servers.
oval:mil.disa.stig.windows2022:def:254339	WN22-CC-000070 - Windows Server 2022 insecure logons to an SMB server must be disabled.
oval:mil.disa.stig.windows2022:def:254340	WN22-CC-000080 - Windows Server 2022 hardened Universal Naming Convention (UNC) paths must be defined to require mutual authentication and integrity for at least the *\SYSVOL and *\NETLOGON shares.
oval:mil.disa.stig.windows2022:def:254341	WN22-CC-000090 - Windows Server 2022 command line data must be included in process creation events.

Oval ID	Title
oval:mil.disa.stig.windows2022:def:254342	WN22-CC-000100 - Windows Server 2022 must be configured to enable Remote host allows delegation of nonexportable credentials.
oval:mil.disa.stig.windows2022:def:254344	WN22-CC-000130 - Windows Server 2022 Early Launch Antimalware, Boot-Start Driver Initialization Policy must prevent boot drivers identified as bad.
oval:mil.disa.stig.defs:def:254344	Early Launch Antimalware, Boot-Start Driver Initialization Policy must prevent boot drivers.
oval:mil.disa.stig.windows2022:def:254345	WN22-CC-000140 - Windows Server 2022 group policy objects must be reprocessed even if they have not changed.
oval:mil.disa.stig.windows2022:def:254346	WN22-CC-000150 - Windows Server 2022 downloading print driver packages over HTTP must be turned off.
oval:mil.disa.stig.windows2022:def:254347	WN22-CC-000160 - Windows Server 2022 printing over HTTP must be turned off.
oval:mil.disa.stig.windows2022:def:254348	WN22-CC-000170 - Windows Server 2022 network selection user interface (UI) must not be displayed on the logon screen.
oval:mil.disa.stig.windows2022:def:254349	WN22-CC-000180 - Windows Server 2022 users must be prompted to authenticate when the system wakes from sleep (on battery).
oval:mil.disa.stig.windows2022:def:254350	WN22-CC-000190 - Windows Server 2022 users must be prompted to authenticate when the system wakes from sleep (plugged in).
oval:mil.disa.stig.windows2022:def:254351	WN22-CC-000200 - Windows Server 2022 Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.
oval:mil.disa.stig.windows2022:def:254352	WN22-CC-000210 - Windows Server 2022 Autoplay must be turned off for nonvolume devices.
oval:mil.disa.stig.windows2022:def:254353	WN22-CC-000220 - Windows Server 2022 default AutoRun behavior must be configured to prevent AutoRun commands.
oval:mil.disa.stig.windows2022:def:254354	WN22-CC-000230 - Windows Server 2022 AutoPlay must be disabled for all drives.
oval:mil.disa.stig.windows2022:def:254355	WN22-CC-000240 - Windows Server 2022 administrator accounts must not be enumerated during elevation.
oval:mil.disa.stig.windows2022:def:254356	WN22-CC-000250 - Windows Server 2022 Telemetry must be configured to Security or Basic.
oval:mil.disa.stig.windows2022:def:254357	WN22-CC-000260 - Windows Server 2022 Windows Update must not obtain updates from other PCs on the internet.
oval:mil.disa.stig.windows2022:def:254358	WN22-CC-000270 - Windows Server 2022 Application event log size must be configured to 32768 KB or greater.
oval:mil.disa.stig.windows2022:def:254359	WN22-CC-000280 - Windows Server 2022 Security event log size must be configured to 196608 KB or greater.
oval:mil.disa.stig.defs:def:254359	Windows Security event log size must be configured to 196608 KB or greater.
oval:mil.disa.stig.windows2022:def:254360	WN22-CC-000290 - Windows Server 2022 System event log size must be configured to 32768 KB or greater.
oval:mil.disa.stig.windows2022:def:254361	WN22-CC-000300 - Windows Server 2022 Microsoft Defender antivirus SmartScreen must be enabled.
oval:mil.disa.stig.windows2022:def:254362	WN22-CC-000310 - Windows Server 2022 Explorer Data Execution Prevention must be enabled.
oval:mil.disa.stig.windows2022:def:254363	WN22-CC-000320 - Windows Server 2022 Turning off File Explorer heap termination on corruption must be disabled.

Oval ID	Title
oval:mil.disa.stig.windows2022:def:254364	WN22-CC-000330 - Windows Server 2022 File Explorer shell protocol must run in protected mode.
oval:mil.disa.stig.windows2022:def:254365	WN22-CC-000340 - Windows Server 2022 must not save passwords in the Remote Desktop Client.
oval:mil.disa.stig.windows2022:def:254366	WN22-CC-000350 - Windows Server 2022 Remote Desktop Services must prevent drive redirection.
oval:mil.disa.stig.windows2022:def:254367	WN22-CC-000360 - Windows Server 2022 Remote Desktop Services must always prompt a client for passwords upon connection.
oval:mil.disa.stig.windows2022:def:254368	WN22-CC-000370 - Windows Server 2022 Remote Desktop Services must require secure Remote Procedure Call (RPC) communications.
oval:mil.disa.stig.windows2022:def:254369	WN22-CC-000380 - Windows Server 2022 Remote Desktop Services must be configured with the client connection encryption set to High Level.
oval:mil.disa.stig.windows2022:def:254370	WN22-CC-000390 - Windows Server 2022 must prevent attachments from being downloaded from RSS feeds.
oval:mil.disa.stig.windows2022:def:254371	WN22-CC-000400 - Windows Server 2022 must disable Basic authentication for RSS feeds over HTTP.
oval:mil.disa.stig.windows2022:def:254372	WN22-CC-000410 - Windows Server 2022 must prevent Indexing of encrypted files.
oval:mil.disa.stig.windows2022:def:254373	WN22-CC-000420 - Windows Server 2022 must prevent users from changing installation options.
oval:mil.disa.stig.windows2022:def:254374	WN22-CC-000430 - Windows Server 2022 must disable the Windows Installer Always install with elevated privileges option.
oval:mil.disa.stig.windows2022:def:254375	WN22-CC-000440 - Windows Server 2022 users must be notified if a web-based program attempts to install software.
oval:mil.disa.stig.windows2022:def:254376	WN22-CC-000450 - Windows Server 2022 must disable automatically signing in the last interactive user after a system-initiated restart.
oval:mil.disa.stig.windows2022:def:254377	WN22-CC-000460 - Windows Server 2022 PowerShell script block logging must be enabled.
oval:mil.disa.stig.windows2022:def:254378	WN22-CC-000470 - Windows Server 2022 Windows Remote Management (WinRM) client must not use Basic authentication.
oval:mil.disa.stig.windows2022:def:254379	WN22-CC-000480 - Windows Server 2022 Windows Remote Management (WinRM) client must not allow unencrypted traffic.
oval:mil.disa.stig.windows2022:def:254380	WN22-CC-000490 - Windows Server 2022 Windows Remote Management (WinRM) client must not use Digest authentication.
oval:mil.disa.stig.windows2022:def:254381	WN22-CC-000500 - Windows Server 2022 Windows Remote Management (WinRM) service must not use Basic authentication.
oval:mil.disa.stig.windows2022:def:254382	WN22-CC-000510 - Windows Server 2022 Windows Remote Management (WinRM) service must not allow unencrypted traffic.
oval:mil.disa.stig.windows2022:def:254383	WN22-CC-000520 - Windows Server 2022 Windows Remote Management (WinRM) service must not store RunAs credentials.
oval:mil.disa.stig.windows2022:def:254384	WN22-CC-000530 - Windows Server 2022 must have PowerShell Transcription enabled.
oval:mil.disa.stig.windows2022:def:254386	WN22-DC-000020 - Windows Server 2022 Kerberos user logon restrictions must be enforced.
oval:mil.disa.stig.defs:def:254386	Windows Kerberos user logon restrictions must be enforced.

Oval ID	Title
oval:mil.disa.stig.windows2022:def:254387	WN22-DC-000030 - Windows Server 2022 Kerberos service ticket maximum lifetime must be limited to 600 minutes or less.
oval:mil.disa.stig.defs:def:254387	Windows Kerberos service ticket maximum lifetime must be limited to 600 minutes or less.
oval:mil.disa.stig.windows2022:def:254388	WN22-DC-000040 - Windows Server 2022 Kerberos user ticket lifetime must be limited to 10 hours or less.
oval:mil.disa.stig.defs:def:254388	Windows Kerberos user ticket lifetime must be limited to 10 hours or less.
oval:mil.disa.stig.windows2022:def:254389	WN22-DC-000050 - Windows Server 2022 Kerberos policy user ticket renewal maximum lifetime must be limited to seven days or less.
oval:mil.disa.stig.defs:def:254389	Windows Kerberos policy user ticket renewal maximum lifetime must be limited to seven days or less.
oval:mil.disa.stig.windows2022:def:254390	WN22-DC-000060 - Windows Server 2022 computer clock synchronization tolerance must be limited to five minutes or less.
oval:mil.disa.stig.defs:def:254390	Windows computer clock synchronization tolerance must be limited to five minutes or less.
oval:mil.disa.stig.windows2022:def:254391	WN22-DC-000070 - Windows Server 2022 permissions on the Active Directory data files must only allow System and Administrators access.
oval:mil.disa.stig.defs:def:254391	Windows permissions on the Active Directory data files must only allow System and Administrators access.
oval:mil.disa.stig.windows2022:def:254407	WN22-DC-000230 - Windows Server 2022 must be configured to audit Account Management - Computer Account Management successes.
oval:mil.disa.stig.defs:def:254407	Windows must be configured to audit Account Management - Computer Account Management successes.
oval:mil.disa.stig.windows2022:def:254408	WN22-DC-000240 - Windows Server 2022 must be configured to audit DS Access - Directory Service Access successes.
oval:mil.disa.stig.defs:def:254408	Windows must be configured to audit DS Access - Directory Service Access successes.
oval:mil.disa.stig.windows2022:def:254409	WN22-DC-000250 - Windows Server 2022 must be configured to audit DS Access - Directory Service Access failures.
oval:mil.disa.stig.defs:def:254409	Windows must be configured to audit DS Access - Directory Service Access failures.
oval:mil.disa.stig.windows2022:def:254410	WN22-DC-000260 - Windows Server 2022 must be configured to audit DS Access - Directory Service Changes successes.
oval:mil.disa.stig.defs:def:254410	Windows must be configured to audit DS Access - Directory Service Changes successes.
oval:mil.disa.stig.windows2022:def:254416	WN22-DC-000320 - Windows Server 2022 domain controllers must require LDAP access signing.
oval:mil.disa.stig.defs:def:254416	Windows domain controllers must require LDAP access signing.
oval:mil.disa.stig.windows2022:def:254417	WN22-DC-000330 - Windows Server 2022 domain controllers must be configured to allow reset of machine account passwords.
oval:mil.disa.stig.defs:def:254417	Windows domain controllers must be configured to allow reset of machine account passwords.
oval:mil.disa.stig.windows2022:def:254418	WN22-DC-000340 - Windows Server 2022 Access this computer from the network user right must only be assigned to the Administrators, Authenticated Users, and Enterprise Domain Controllers groups on domain controllers.

Oval ID	Title
oval:mil.disa.stig.defs:def:254418	Windows Access this computer from the network user right must only be assigned to the Administrators, Authenticated Users, and Enterprise Domain Controllers groups on domain controllers.
oval:mil.disa.stig.windows2022:def:254419	WN22-DC-000350 - Windows Server 2022 Add workstations to domain user right must only be assigned to the Administrators group on domain controllers.
oval:mil.disa.stig.defs:def:254419	Windows Add workstations to domain user right must only be assigned to the Administrators group on domain controllers.
oval:mil.disa.stig.windows2022:def:254420	WN22-DC-000360 - Windows Server 2022 Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group on domain controllers.
oval:mil.disa.stig.defs:def:254420	Windows Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group on domain controllers.
oval:mil.disa.stig.windows2022:def:254421	WN22-DC-000370 - Windows Server 2022 Deny access to this computer from the network user right on domain controllers must be configured to prevent unauthenticated access.
oval:mil.disa.stig.defs:def:254421	Windows Deny access to this computer from the network user right on domain controllers must be configured to prevent unauthenticated access.
oval:mil.disa.stig.windows2022:def:254422	WN22-DC-000380 - Windows Server 2022 Deny log on as a batch job user right on domain controllers must be configured to prevent unauthenticated access.
oval:mil.disa.stig.defs:def:254422	Windows Deny log on as a batch job user right on domain controllers must be configured to prevent unauthenticated access.
oval:mil.disa.stig.windows2022:def:254423	WN22-DC-000390 - Windows Server 2022 Deny log on as a service user right must be configured to include no accounts or groups (blank) on domain controllers.
oval:mil.disa.stig.defs:def:254423	Windows Deny log on as a service user right must be configured to include no accounts or groups (blank) on domain controllers.
oval:mil.disa.stig.windows2022:def:254424	WN22-DC-000400 - Windows Server 2022 Deny log on locally user right on domain controllers must be configured to prevent unauthenticated access.
oval:mil.disa.stig.defs:def:254424	Windows Deny log on locally user right on domain controllers must be configured to prevent unauthenticated access.
oval:mil.disa.stig.windows2022:def:254425	WN22-DC-000410 - Windows Server 2022 Deny log on through Remote Desktop Services user right on domain controllers must be configured to prevent unauthenticated access.
oval:mil.disa.stig.defs:def:254425	Windows Deny log on through Remote Desktop Services user right on domain controllers must be configured to prevent unauthenticated access.
oval:mil.disa.stig.windows2022:def:254426	WN22-DC-000420 - Windows Server 2022 Enable computer and user accounts to be trusted for delegation user right must only be assigned to the Administrators group on domain controllers.
oval:mil.disa.stig.defs:def:254426	Windows Enable computer and user accounts to be trusted for delegation user right must only be assigned to the Administrators group on domain controllers.
oval:mil.disa.stig.windows2022:def:254429	WN22-MS-000020 - Windows Server 2022 local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain-joined member servers.
oval:mil.disa.stig.windows2022:def:254430	WN22-MS-000030 - Windows Server 2022 local users on domain-joined member servers must not be enumerated.
oval:mil.disa.stig.windows2022:def:254431	WN22-MS-000040 - Windows Server 2022 must restrict unauthenticated Remote Procedure Call (RPC) clients from connecting to the RPC server on domain-joined member servers and standalone or nondomain-joined systems.

Oval ID	Title
oval:mil.disa.stig.windows2022:def:254432	WN22-MS-000050 - Windows Server 2022 must limit the caching of logon credentials to four or less on domain-joined member servers.
oval:mil.disa.stig.defs:def:254432	Windows must limit the caching of logon credentials to four or less on domain-joined member servers.
oval:mil.disa.stig.windows2022:def:254433	WN22-MS-000060 - Windows Server 2022 must restrict remote calls to the Security Account Manager (SAM) to Administrators on domain-joined member servers and standalone or nondomain-joined systems.
oval:mil.disa.stig.windows2022:def:254434	WN22-MS-000070 - Windows Server 2022 Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on domain-joined member servers and standalone or nondomain-joined systems.
oval:mil.disa.stig.defs:def:254434	Windows Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on domain-joined member servers and standalone or nondomain-joined systems.
oval:mil.disa.stig.windows2022:def:254435	WN22-MS-000080 - Windows Server 2022 Deny access to this computer from the network user right on domain-joined member servers must be configured to prevent access from highly privileged domain accounts and local accounts and from unauthenticated access on all systems.
oval:mil.disa.stig.defs:def:254435	Windows Deny access to this computer from the network user right on domain-joined member servers must be configured to prevent access from highly privileged domain accounts and local accounts and from unauthenticated access on all systems.
oval:mil.disa.stig.windows2022:def:254436	WN22-MS-000090 - Windows Server 2022 Deny log on as a batch job user right on domain-joined member servers must be configured to prevent access from highly privileged domain accounts and from unauthenticated access on all systems.
oval:mil.disa.stig.defs:def:254436	Windows Deny log on as a batch job user right on domain-joined member servers must be configured to prevent access from highly privileged domain accounts and from unauthenticated access on all systems.
oval:mil.disa.stig.windows2022:def:254437	WN22-MS-000100 - Windows Server 2022 Deny log on as a service user right on domain-joined member servers must be configured to prevent access from highly privileged domain accounts. No other groups or accounts must be assigned this right.
oval:mil.disa.stig.windows2022:def:254438	WN22-MS-000110 - Windows Server 2022 Deny log on locally user right on domain-joined member servers must be configured to prevent access from highly privileged domain accounts and from unauthenticated access on all systems.
oval:mil.disa.stig.windows2022:def:254439	WN22-MS-000120 - Windows Server 2022 Deny log on through Remote Desktop Services user right on domain-joined member servers must be configured to prevent access from highly privileged domain accounts and all local accounts and from unauthenticated access on all systems.
oval:mil.disa.stig.defs:def:254439	The "Deny log on through Remote Desktop Services" user right on domain-joined member servers must be configured to prevent access from highly privileged domain accounts and all local accounts and from unauthenticated access on all systems.
oval:mil.disa.stig.windows2022:def:254440	WN22-MS-000130 - Windows Server 2022 Enable computer and user accounts to be trusted for delegation user right must not be assigned to any groups or accounts on domain-joined member servers and standalone or nondomain-joined systems.
oval:mil.disa.stig.windows2022:def:254442	WN22-PK-000010 - Windows Server 2022 must have the DoD Root Certificate Authority (CA) certificates installed in the Trusted Root Store.

Oval ID	Title
oval:mil.disa.stig.windows2022:def:254443	WN22-PK-000020 - Windows Server 2022 must have the DoD Interoperability Root Certificate Authority (CA) cross-certificates installed in the Untrusted Certificates Store on unclassified systems.
oval:mil.disa.stig.windows2022:def:254444	WN22-PK-000030 - Windows Server 2022 must have the US DoD CCEB Interoperability Root CA cross-certificates in the Untrusted Certificates Store on unclassified systems.
oval:mil.disa.stig.windows2022:def:254445	WN22-SO-000010 - Windows Server 2022 must have the built-in guest account disabled.
oval:mil.disa.stig.windows2022:def:254446	WN22-SO-000020 - Windows Server 2022 must prevent local accounts with blank passwords from being used from the network.
oval:mil.disa.stig.windows2022:def:254447	WN22-SO-000030 - Windows Server 2022 built-in administrator account must be renamed.
oval:mil.disa.stig.windows2022:def:254448	WN22-SO-000040 - Windows Server 2022 built-in guest account must be renamed.
oval:mil.disa.stig.windows2022:def:254449	WN22-SO-000050 - Windows Server 2022 must force audit policy subcategory settings to override audit policy category settings.
oval:mil.disa.stig.windows2022:def:254450	WN22-SO-000060 - Windows Server 2022 setting Domain member: Digitally encrypt or sign secure channel data (always) must be configured to Enabled.
oval:mil.disa.stig.windows2022:def:254451	WN22-SO-000070 - Windows Server 2022 setting Domain member: Digitally encrypt secure channel data (when possible) must be configured to Enabled.
oval:mil.disa.stig.windows2022:def:254452	WN22-SO-000080 - Windows Server 2022 setting Domain member: Digitally sign secure channel data (when possible) must be configured to Enabled.
oval:mil.disa.stig.windows2022:def:254453	WN22-SO-000090 - Windows Server 2022 computer account password must not be prevented from being reset.
oval:mil.disa.stig.windows2022:def:254454	WN22-SO-000100 - Windows Server 2022 maximum age for machine account passwords must be configured to 30 days or less.
oval:mil.disa.stig.windows2022:def:254455	WN22-SO-000110 - Windows Server 2022 must be configured to require a strong session key.
oval:mil.disa.stig.windows2022:def:254456	WN22-SO-000120 - Windows Server 2022 machine inactivity limit must be set to 15 minutes or less, locking the system with the screen saver.
oval:mil.disa.stig.windows2022:def:254459	WN22-SO-000150 - Windows Server 2022 Smart Card removal option must be configured to Force Logoff or Lock Workstation.
oval:mil.disa.stig.windows2022:def:254460	WN22-SO-000160 - Windows Server 2022 setting Microsoft network client: Digitally sign communications (always) must be configured to Enabled.
oval:mil.disa.stig.windows2022:def:254461	WN22-SO-000170 - Windows Server 2022 setting Microsoft network client: Digitally sign communications (if server agrees) must be configured to Enabled.
oval:mil.disa.stig.defs:def:254461	Windows setting Microsoft network client: Digitally sign communications (if server agrees) must be configured to Enabled.
oval:mil.disa.stig.windows2022:def:254462	WN22-SO-000180 - Windows Server 2022 unencrypted passwords must not be sent to third-party Server Message Block (SMB) servers.
oval:mil.disa.stig.windows2022:def:254463	WN22-SO-000190 - Windows Server 2022 setting Microsoft network server: Digitally sign communications (always) must be configured to Enabled.
oval:mil.disa.stig.windows2022:def:254464	WN22-SO-000200 - Windows Server 2022 setting Microsoft network server: Digitally sign communications (if client agrees) must be configured to Enabled.
oval:mil.disa.stig.defs:def:254464	Windows setting Microsoft network server: Digitally sign communications (if client agrees) must be configured to Enabled.

Oval ID	Title
oval:mil.disa.stig.windows2022:def:254466	WN22-SO-000220 - Windows Server 2022 must not allow anonymous enumeration of Security Account Manager (SAM) accounts.
oval:mil.disa.stig.windows2022:def:254467	WN22-SO-000230 - Windows Server 2022 must not allow anonymous enumeration of shares.
oval:mil.disa.stig.windows2022:def:254468	WN22-SO-000240 - Windows Server 2022 must be configured to prevent anonymous users from having the same permissions as the Everyone group.
oval:mil.disa.stig.windows2022:def:254469	WN22-SO-000250 - Windows Server 2022 must restrict anonymous access to Named Pipes and Shares.
oval:mil.disa.stig.windows2022:def:254470	WN22-SO-000260 - Windows Server 2022 services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity instead of authenticating anonymously.
oval:mil.disa.stig.defs:def:254470	Windows services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity instead of authenticating anonymously.
oval:mil.disa.stig.windows2022:def:254471	WN22-SO-000270 - Windows Server 2022 must prevent NTLM from falling back to a Null session.
oval:mil.disa.stig.windows2022:def:254472	WN22-SO-000280 - Windows Server 2022 must prevent PKU2U authentication using online identities.
oval:mil.disa.stig.windows2022:def:254473	WN22-SO-000290 - Windows Server 2022 Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.
oval:mil.disa.stig.windows2022:def:254474	WN22-SO-000300 - Windows Server 2022 must be configured to prevent the storage of the LAN Manager hash of passwords.
oval:mil.disa.stig.windows2022:def:254475	WN22-SO-000310 - Windows Server 2022 LAN Manager authentication level must be configured to send NTLMv2 response only and to refuse LM and NTLM.
oval:mil.disa.stig.windows2022:def:254476	WN22-SO-000320 - Windows Server 2022 must be configured to at least negotiate signing for LDAP client signing.
oval:mil.disa.stig.windows2022:def:254477	WN22-SO-000330 - Windows Server 2022 session security for NTLM SSP-based clients must be configured to require NTLMv2 session security and 128-bit encryption.
oval:mil.disa.stig.windows2022:def:254478	WN22-SO-000340 - Windows Server 2022 session security for NTLM SSP-based servers must be configured to require NTLMv2 session security and 128-bit encryption.
oval:mil.disa.stig.windows2022:def:254479	WN22-SO-000350 - Windows Server 2022 users must be required to enter a password to access private keys stored on the computer.
oval:mil.disa.stig.defs:def:254479	Windows users must be required to enter a password to access private keys stored on the computer.
oval:mil.disa.stig.windows2022:def:254480	WN22-SO-000360 - Windows Server 2022 must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.
oval:mil.disa.stig.windows2022:def:254481	WN22-SO-000370 - Windows Server 2022 default permissions of global system objects must be strengthened.
oval:mil.disa.stig.windows2022:def:254482	WN22-SO-000380 - Windows Server 2022 User Account Control (UAC) approval mode for the built-in Administrator must be enabled.
oval:mil.disa.stig.windows2022:def:254483	WN22-SO-000390 - Windows Server 2022 UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.
oval:mil.disa.stig.defs:def:254483	Windows UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.

Oval ID	Title
oval:mil.disa.stig.windows2022:def:254484	WN22-SO-000400 - Windows Server 2022 User Account Control (UAC) must, at a minimum, prompt administrators for consent on the secure desktop.
oval:mil.disa.stig.defs:def:254484	Windows User Account Control (UAC) must, at a minimum, prompt administrators for consent on the secure desktop.
oval:mil.disa.stig.windows2022:def:254485	WN22-SO-000410 - Windows Server 2022 User Account Control (UAC) must automatically deny standard user requests for elevation.
oval:mil.disa.stig.windows2022:def:254486	WN22-SO-000420 - Windows Server 2022 User Account Control (UAC) must be configured to detect application installations and prompt for elevation.
oval:mil.disa.stig.windows2022:def:254487	WN22-SO-000430 - Windows Server 2022 User Account Control (UAC) must only elevate UIAccess applications that are installed in secure locations.
oval:mil.disa.stig.windows2022:def:254488	WN22-SO-000440 - Windows Server 2022 User Account Control (UAC) must run all administrators in Admin Approval Mode, enabling UAC.
oval:mil.disa.stig.windows2022:def:254489	WN22-SO-000450 - Windows Server 2022 User Account Control (UAC) must virtualize file and registry write failures to per-user locations.
oval:mil.disa.stig.windows2022:def:254491	WN22-UR-000010 - Windows Server 2022 Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.
oval:mil.disa.stig.windows2022:def:254492	WN22-UR-000020 - Windows Server 2022 Act as part of the operating system user right must not be assigned to any groups or accounts.
oval:mil.disa.stig.windows2022:def:254493	WN22-UR-000030 - Windows Server 2022 Allow log on locally user right must only be assigned to the Administrators group.
oval:mil.disa.stig.defs:def:254493	Windows Allow log on locally user right must only be assigned to the Administrators group.
oval:mil.disa.stig.windows2022:def:254494	WN22-UR-000040 - Windows Server 2022 back up files and directories user right must only be assigned to the Administrators group.
oval:mil.disa.stig.windows2022:def:254495	WN22-UR-000050 - Windows Server 2022 create a pagefile user right must only be assigned to the Administrators group.
oval:mil.disa.stig.windows2022:def:254496	WN22-UR-000060 - Windows Server 2022 create a token object user right must not be assigned to any groups or accounts.
oval:mil.disa.stig.windows2022:def:254497	WN22-UR-000070 - Windows Server 2022 create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.
oval:mil.disa.stig.windows2022:def:254498	WN22-UR-000080 - Windows Server 2022 create permanent shared objects user right must not be assigned to any groups or accounts.
oval:mil.disa.stig.windows2022:def:254499	WN22-UR-000090 - Windows Server 2022 create symbolic links user right must only be assigned to the Administrators group.
oval:mil.disa.stig.defs:def:254499	The "Create symbolic links" user right must only be assigned to the Administrators group.
oval:mil.disa.stig.windows2022:def:254500	WN22-UR-000100 - Windows Server 2022 debug programs user right must only be assigned to the Administrators group.
oval:mil.disa.stig.windows2022:def:254501	WN22-UR-000110 - Windows Server 2022 force shutdown from a remote system user right must only be assigned to the Administrators group.
oval:mil.disa.stig.windows2022:def:254502	WN22-UR-000120 - Windows Server 2022 generate security audits user right must only be assigned to Local Service and Network Service.
oval:mil.disa.stig.defs:def:254502	Windows generate security audits user right must only be assigned to Local Service and Network Service.

Oval ID	Title
oval:mil.disa.stig.windows2022:def:254503	WN22-UR-000130 - Windows Server 2022 impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.
oval:mil.disa.stig.windows2022:def:254504	WN22-UR-000140 - Windows Server 2022 increase scheduling priority: user right must only be assigned to the Administrators group.
oval:mil.disa.stig.defs:def:254504	Windows increase scheduling priority: user right must only be assigned to the Administrators group.
oval:mil.disa.stig.windows2022:def:254505	WN22-UR-000150 - Windows Server 2022 load and unload device drivers user right must only be assigned to the Administrators group.
oval:mil.disa.stig.windows2022:def:254506	WN22-UR-000160 - Windows Server 2022 lock pages in memory user right must not be assigned to any groups or accounts.
oval:mil.disa.stig.windows2022:def:254507	WN22-UR-000170 - Windows Server 2022 manage auditing and security log user right must only be assigned to the Administrators group.
oval:mil.disa.stig.windows2022:def:254508	WN22-UR-000180 - Windows Server 2022 modify firmware environment values user right must only be assigned to the Administrators group.
oval:mil.disa.stig.windows2022:def:254509	WN22-UR-000190 - Windows Server 2022 perform volume maintenance tasks user right must only be assigned to the Administrators group.
oval:mil.disa.stig.windows2022:def:254510	WN22-UR-000200 - Windows Server 2022 profile single process user right must only be assigned to the Administrators group.
oval:mil.disa.stig.windows2022:def:254511	WN22-UR-000210 - Windows Server 2022 restore files and directories user right must only be assigned to the Administrators group.
oval:mil.disa.stig.windows2022:def:254512	WN22-UR-000220 - Windows Server 2022 take ownership of files or other objects user right must only be assigned to the Administrators group.
oval:mil.disa.stig.windows10:def:220745	WN10-AC-000035 - Passwords must, at a minimum, be 14 characters.
oval:mil.disa.stig.windows10:def:220706	WN10-00-000040 - Windows 10 systems must be maintained at a supported servicing level.
oval:mil.disa.stig.defs:def:220706	Windows systems must be maintained at a supported servicing level.
oval:mil.disa.stig.windows10:def:220835	WN10-CC-000206 - Windows Update must not obtain updates from other PCs on the internet.
oval:mil.disa.stig.defs:def:220835	Windows Update for workstations must not obtain updates from other PCs on the internet or be running Windows 10 LTSB v1507.
oval:mil.disa.stig.rhel8os:def:230244	RHEL-08-010200 - RHEL 8 must be configured so that all network connections associated with SSH traffic are terminated at the end of the session or after 10 minutes of inactivity, except to fulfill documented and validated mission requirements.
oval:mil.disa.stig.rhel8os:def:230257	RHEL-08-010300 - RHEL 8 system commands must have mode 755 or less permissive.
oval:mil.disa.stig.rhel8os:def:230292	RHEL-08-010540 - RHEL 8 must use a separate file system for /var.
oval:mil.disa.stig.rhel8os:def:230293	RHEL-08-010541 - RHEL 8 must use a separate file system for /var/log.
oval:mil.disa.stig.rhel8os:def:230346	RHEL-08-020024 - RHEL 8 must limit the number of concurrent sessions to ten for all accounts and/or account types.
oval:mil.disa.stig.rhel8os:def:230356	RHEL-08-020100 - RHEL 8 must ensure the password complexity module is enabled in the password-auth file.
oval:mil.disa.stig.rhel8os:def:230396	RHEL-08-030070 - RHEL 8 audit logs must have a mode of 0600 or less permissive to prevent unauthorized read access.

Oval ID	Title
oval:mil.disa.stig.windows2019:def:205633	WN19-SO-000120 - Windows Server 2019 machine inactivity limit must be set to 15 minutes or less, locking the system with the screen saver.
oval:mil.disa.stig.windows2019:def:205640	WN19-AU-000030 - Windows Server 2019 permissions for the Application event log must prevent access by non-privileged accounts.
oval:mil.disa.stig.windows2019:def:205641	WN19-AU-000040 - Windows Server 2019 permissions for the Security event log must prevent access by non-privileged accounts.
oval:mil.disa.stig.windows2019:def:205642	WN19-AU-000050 - Windows Server 2019 permissions for the System event log must prevent access by non-privileged accounts.
oval:mil.disa.stig.windows2019:def:205648	WN19-PK-000010 - Windows Server 2019 must have the DoD Root Certificate Authority (CA) certificates installed in the Trusted Root Store.
oval:mil.disa.stig.windows2019:def:205649	WN19-PK-000020 - Windows Server 2019 must have the DoD Interoperability Root Certificate Authority (CA) cross-certificates installed in the Untrusted Certificates Store on unclassified systems.
oval:mil.disa.stig.windows2019:def:205650	WN19-PK-000030 - Windows Server 2019 must have the US DoD CCEB Interoperability Root CA cross-certificates in the Untrusted Certificates Store on unclassified systems.
oval:mil.disa.stig.windows2019:def:205662	WN19-AC-000070 - Windows Server 2019 minimum password length must be configured to 14 characters.
oval:mil.disa.stig.windows2019:def:205674	WN19-MS-000100 - Windows Server 2019 "Deny log on as a service" user right on domain-joined member servers must be configured to prevent access from highly privileged domain accounts. No other groups or accounts must be assigned this right.
oval:mil.disa.stig.windows2019:def:205731	WN19-AU-000060 - Windows Server 2019 Event Viewer must be protected from unauthorized modification and deletion.
oval:mil.disa.stig.windows2019:def:205739	WN19-DC-000070 - Windows Server 2019 permissions on the Active Directory data files must only allow System and Administrators access.
oval:mil.disa.stig.windows2019:def:205765	WN19-UR-000190 - Windows Server 2019 Perform volume maintenance tasks user right must only be assigned to the Administrators group.
oval:mil.disa.stig.windows2019:def:205869	WN19-CC-000250 - Windows Server 2019 Telemetry must be configured to Security or Basic.
oval:mil.disa.stig.windows10:def:220806	WN10-CC-000055 - Simultaneous connections to the internet or a Windows domain must be limited.
oval:mil.disa.stig.windows10:def:220834	WN10-CC-000205 - Windows Telemetry must not be configured to Full.
oval:mil.disa.stig.windows10:def:220903	WN10-PK-000005 - The DoD Root CA certificates must be installed in the Trusted Root Store.
oval:mil.disa.stig.windows10:def:220904	WN10-PK-000010 - The External Root CA certificates must be installed in the Trusted Root Store on unclassified systems.
oval:mil.disa.stig.windows10:def:220905	WN10-PK-000015 - The DoD Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.
oval:mil.disa.stig.windows10:def:220906	WN10-PK-000020 - The US DoD CCEB Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.
oval:mil.disa.stig.windows10:def:220920	WN10-SO-000070 - The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.
oval:mil.disa.stig.windows10:def:220946	WN10-SO-000251 - Windows 10 must use multifactor authentication for local and network access to privileged and non-privileged accounts.

Oval ID	Title
oval:mil.disa.stig.windows10:def:220970	WN10-UR-000080 - The Deny log on as a service user right on Windows 10 domain-joined workstations must be configured to prevent access from highly privileged domain accounts.
oval:mil.disa.stig.windows10:def:220980	WN10-UR-000145 - The Perform volume maintenance tasks user right must only be assigned to the Administrators group.
oval:mil.disa.stig.windows10:def:256894	WN10-CC-000391 - Internet Explorer must be disabled for Windows 10.
oval:mil.disa.stig.defs:def:256893	Internet Explorer must be disabled for Windows.
oval:mil.disa.stig.defs:def:254356	Windows Telemetry must not be configured to Full.
oval:mil.disa.stig.windows11:def:256893	WN11-CC-000391 - Internet Explorer must be disabled for Windows 11.
oval:mil.disa.stig.rhel8os:def:230221	RHEL-08-010000 - RHEL 8 must be a vendor-supported release.
oval:mil.disa.stig.rhel8os:def:230265	RHEL-08-010371 - RHEL 8 must prevent the installation of software, patches, service packs, device drivers, or operating system components of local packages without verification they have been digitally signed using a certificate that is issued by a Certificate Authority (CA) that is recognized and approved by the organization.
oval:mil.disa.stig.rhel8os:def:230357	RHEL-08-020110 - RHEL 8 must enforce password complexity by requiring that at least one uppercase character be used.
oval:mil.disa.stig.rhel8os:def:230358	RHEL-08-020120 - RHEL 8 must enforce password complexity by requiring that at least one lower-case character be used.
oval:mil.disa.stig.rhel8os:def:230359	RHEL-08-020130 - RHEL 8 must enforce password complexity by requiring that at least one numeric character be used.
oval:mil.disa.stig.rhel8os:def:230360	RHEL-08-020140 - RHEL 8 must require the maximum number of repeating characters of the same character class be limited to four when passwords are changed.
oval:mil.disa.stig.rhel8os:def:230361	RHEL-08-020150 - RHEL 8 must require the maximum number of repeating characters be limited to three when passwords are changed.
oval:mil.disa.stig.rhel8os:def:230362	RHEL-08-020160 - RHEL 8 must require the change of at least four character classes when passwords are changed.
oval:mil.disa.stig.rhel8os:def:230363	RHEL-08-020170 - RHEL 8 must require the change of at least 8 characters when passwords are changed.
oval:mil.disa.stig.rhel8os:def:230369	RHEL-08-020230 - RHEL 8 passwords must have a minimum of 15 characters.
oval:mil.disa.stig.rhel8os:def:230375	RHEL-08-020280 - All RHEL 8 passwords must contain at least one special character.
oval:mil.disa.stig.rhel8os:def:230381	RHEL-08-020340 - RHEL 8 must display the date and time of the last successful account logon upon logon.
oval:mil.disa.stig.windows10:def:220754	WN10-AU-000050 - The system must be configured to audit Detailed Tracking - Process Creation successes.
oval:mil.disa.stig.defs:def:220834	Windows Telemetry is configured to Enhanced.
oval:mil.disa.stig.windows10:def:252896	WN10-CC-000327 - PowerShell Transcription must be enabled on Windows 10.
oval:mil.disa.stig.windows10:def:257589	WN10-AU-000585 - Windows 10 must have command line process auditing events enabled.
oval:mil.disa.stig.defs:def:257770	The system must be configured to audit Detailed Tracking - Process Creation failures.

Oval ID	Title
oval:mil.disa.stig.windows2019:def:257503	WN19-CC-000530 - Windows Server 2019 must have PowerShell Transcription enabled.
oval:mil.disa.stig.windows11:def:257770	WN11-AU-000585 - Windows 11 must have command line process auditing events enabled.
oval:mil.disa.stig.rhel8os:def:230237	RHEL-08-010160 - The RHEL 8 pam_unix.so module must be configured in the password-auth file to use a FIPS 140-2 approved cryptographic hashing algorithm for system authentication.
oval:mil.disa.stig.rhel8os:def:230367	RHEL-08-020210 - RHEL 8 user account passwords must be configured so that existing passwords are restricted to a 60-day maximum lifetime.
oval:mil.disa.stig.rhel8os:def:230376	RHEL-08-020290 - RHEL 8 must prohibit the use of cached authentications after one day.
oval:mil.disa.stig.rhel8os:def:230494	RHEL-08-040021 - RHEL 8 must disable the asynchronous transfer mode (ATM) protocol.
oval:mil.disa.stig.rhel8os:def:230495	RHEL-08-040022 - RHEL 8 must disable the controller area network (CAN) protocol.
oval:mil.disa.stig.rhel8os:def:230496	RHEL-08-040023 - RHEL 8 must disable the stream control transmission protocol (SCTP).
oval:mil.disa.stig.rhel8os:def:230497	RHEL-08-040024 - RHEL 8 must disable the transparent inter-process communication (TIPC) protocol.
oval:mil.disa.stig.rhel8os:def:230498	RHEL-08-040025 - RHEL 8 must disable mounting of cramfs.
oval:mil.disa.stig.rhel8os:def:230499	RHEL-08-040026 - RHEL 8 must disable IEEE 1394 (FireWire) Support.
oval:mil.disa.stig.rhel8os:def:230503	RHEL-08-040080 - RHEL 8 must be configured to disable USB mass storage.
oval:mil.disa.stig.rhel8os:def:230507	RHEL-08-040111 - RHEL 8 Bluetooth must be disabled.
oval:mil.disa.stig.rhel8os:def:244524	RHEL-08-010159 - The RHEL 8 pam_unix.so module must be configured in the system-auth file to use a FIPS 140-2 approved cryptographic hashing algorithm for system authentication.
oval:mil.disa.stig.rhel8os:def:257258	RHEL-08-020035 - RHEL 8 must terminate idle user sessions.
oval:mil.disa.stig.rhel9os:def:1	RHEL 9 is installed
oval:mil.disa.stig.defs:def:230269	The operating system must restrict access to the kernel message buffer.
oval:mil.disa.stig.defs:def:230311	The operating system must disable the kernel.core_pattern.
oval:mil.disa.stig.linux:def:100007	Linux BIOS
oval:mil.disa.stig.defs:def:25785400	The system has nfs entries in /etc/fstab
oval:mil.disa.stig.defs:def:25823200	The libreswan package is installed.
oval:mil.disa.stig.defs:def:25824200	The system has BIND installed.
oval:mil.disa.stig.defs:def:230280	The operating system must implement address space layout randomization (ASLR) to protect its memory from unauthorized code execution.
oval:mil.disa.stig.rhel9os:def:257884	RHEL-09-232020 - RHEL 9 library files must have mode 755 or less permissive.
oval:mil.disa.stig.defs:def:257959	The operating system must not forward IPv4 source-routed packets.
oval:mil.disa.stig.defs:def:257961	The operating system must log IPv4 packets with impossible addresses by default.
oval:mil.disa.stig.defs:def:230549	The operating system must use reverse path filtering on all IPv4 interfaces.

Oval ID	Title
oval:mil.disa.stig.defs:def:204611	The operating system must use a reverse-path filter for IPv4 network traffic when possible by default.
oval:mil.disa.stig.defs:def:257967	The operating system must limit the number of bogus Internet Control Message Protocol (ICMP) response errors logs.
oval:mil.disa.stig.defs:def:230536	The operating system must not send Internet Control Message Protocol (ICMP) redirects.
oval:mil.disa.stig.defs:def:257971	The operating system must not accept router advertisements on all IPv6 interfaces.
oval:mil.disa.stig.defs:def:230540	The operating system must not enable IPv6 packet forwarding unless the system is a router.
oval:mil.disa.stig.rhel9os:def:258129	RHEL-09-611200 - RHEL 9 must require authentication to access single-user mode.
oval:mil.disa.stig.defs:def:230483	The operating system must take action when allocated audit record storage volume reaches 75 percent of the repository maximum audit record storage capacity.
oval:mil.disa.stig.defs:def:230439	Successful/unsuccessful uses of the rename, unlink, rmdir, renameat, and unlinkat system calls in the operating system must generate an audit record.
oval:mil.disa.stig.defs:def:25784900	The autofs package is installed.
oval:mil.disa.stig.defs:def:25795100	The postifx package is installed.
oval:mil.disa.stig.rhel8os:def:230559	RHEL-08-040370 - The gssproxy package must not be installed unless mission essential on RHEL 8.
oval:mil.disa.stig.windows2019:def:205638	WN19-CC-000090 - Windows Server 2019 command line data must be included in process creation events.
oval:mil.disa.stig.windows10:def:220809	WN10-CC-000066 - Command line data must be included in process creation events.
oval:mil.disa.stig.linux:def:100015	krb5 workstation 1.17 or higher
oval:mil.disa.stig.linux:def:100014	krb5 server 1.17 or higher
oval:mil.disa.stig.defs:def:25795200	The Trivial File Transfer Protocol (TFTP) server package is installed.
oval:mil.disa.stig.linux:def:100001	The system is RHEL 8.1 or lower
oval:mil.disa.stig.linux:def:100002	The system is RHEL 8.2 or higher
oval:mil.disa.stig.rhel8os:def:230228	RHEL-08-010070 - All RHEL 8 remote access methods must be monitored.
oval:mil.disa.stig.rhel8os:def:230231	RHEL-08-010110 - RHEL 8 must encrypt all stored passwords with a FIPS 140-2 approved cryptographic hashing algorithm.
oval:mil.disa.stig.rhel8os:def:230232	RHEL-08-010120 - RHEL 8 must employ FIPS 140-2 approved cryptographic hashing algorithms for all stored passwords.
oval:mil.disa.stig.rhel8os:def:230233	RHEL-08-010130 - The RHEL 8 shadow password suite must be configured to use a sufficient number of hashing rounds.
oval:mil.disa.stig.rhel8os:def:230234	RHEL-08-010140 - RHEL 8 operating systems booted with United Extensible Firmware Interface (UEFI) must require authentication upon booting into single-user mode and maintenance.
oval:mil.disa.stig.rhel8os:def:230235	RHEL-08-010150 - RHEL 8 operating systems booted with a BIOS must require authentication upon booting into single-user and maintenance modes.

Oval ID	Title
oval:mil.disa.stig.rhel8os:def:230236	RHEL-08-010151 - RHEL 8 operating systems must require authentication upon booting into rescue mode.
oval:mil.disa.stig.rhel8os:def:230238	RHEL-08-010161 - RHEL 8 must prevent system daemons from using Kerberos for authentication.
oval:mil.disa.stig.rhel8os:def:230239	RHEL-08-010162 - The krb5-workstation package must not be installed on RHEL 8.
oval:mil.disa.stig.rhel8os:def:230241	RHEL-08-010171 - RHEL 8 must have policycoreutils package installed.
oval:mil.disa.stig.rhel8os:def:230245	RHEL-08-010210 - The RHEL 8 /var/log/messages file must have mode 0640 or less permissive.
oval:mil.disa.stig.rhel8os:def:230246	RHEL-08-010220 - The RHEL 8 /var/log/messages file must be owned by root.
oval:mil.disa.stig.rhel8os:def:230247	RHEL-08-010230 - The RHEL 8 /var/log/messages file must be group-owned by root.
oval:mil.disa.stig.rhel8os:def:230248	RHEL-08-010240 - The RHEL 8 /var/log directory must have mode 0755 or less permissive.
oval:mil.disa.stig.rhel8os:def:230249	RHEL-08-010250 - The RHEL 8 /var/log directory must be owned by root.
oval:mil.disa.stig.rhel8os:def:230250	RHEL-08-010260 - The RHEL 8 /var/log directory must be group-owned by root.
oval:mil.disa.stig.rhel8os:def:230253	RHEL-08-010292 - RHEL 8 must ensure the SSH server uses strong entropy.
oval:mil.disa.stig.rhel8os:def:230255	RHEL-08-010294 - The RHEL 8 operating system must implement DoD-approved TLS encryption in the OpenSSL package.
oval:mil.disa.stig.rhel8os:def:230258	RHEL-08-010310 - RHEL 8 system commands must be owned by root.
oval:mil.disa.stig.rhel8os:def:230259	RHEL-08-010320 - RHEL 8 system commands must be group-owned by root or a system account.
oval:mil.disa.stig.rhel8os:def:230260	RHEL-08-010330 - RHEL 8 library files must have mode 755 or less permissive.
oval:mil.disa.stig.rhel8os:def:230261	RHEL-08-010340 - RHEL 8 library files must be owned by root.
oval:mil.disa.stig.rhel8os:def:230262	RHEL-08-010350 - RHEL 8 library files must be group-owned by root or a system account.
oval:mil.disa.stig.rhel8os:def:230264	RHEL-08-010370 - RHEL 8 must prevent the installation of software, patches, service packs, device drivers, or operating system components from a repository without verification they have been digitally signed using a certificate that is issued by a Certificate Authority (CA) that is recognized and approved by the organization.
oval:mil.disa.stig.rhel8os:def:230266	RHEL-08-010372 - RHEL 8 must prevent the loading of a new kernel for later execution.
oval:mil.disa.stig.rhel8os:def:230267	RHEL-08-010373 - RHEL 8 must enable kernel parameters to enforce discretionary access control on symlinks.
oval:mil.disa.stig.rhel8os:def:230268	RHEL-08-010374 - RHEL 8 must enable kernel parameters to enforce discretionary access control on hardlinks.
oval:mil.disa.stig.rhel8os:def:230269	RHEL-08-010375 - RHEL 8 must restrict access to the kernel message buffer.
oval:mil.disa.stig.rhel8os:def:230270	RHEL-08-010376 - RHEL 8 must prevent kernel profiling by unprivileged users.
oval:mil.disa.stig.rhel8os:def:230271	RHEL-08-010380 - RHEL 8 must require users to provide a password for privilege escalation.
oval:mil.disa.stig.rhel8os:def:230272	RHEL-08-010381 - RHEL 8 must require users to reauthenticate for privilege escalation.

Oval ID	Title
oval:mil.disa.stig.rhel8os:def:230273	RHEL-08-010390 - RHEL 8 must have the packages required for multifactor authentication installed.
oval:mil.disa.stig.rhel8os:def:230280	RHEL-08-010430 - RHEL 8 must implement address space layout randomization (ASLR) to protect its memory from unauthorized code execution.
oval:mil.disa.stig.rhel8os:def:230281	RHEL-08-010440 - YUM must remove all software components after updated versions have been installed on RHEL 8.
oval:mil.disa.stig.rhel8os:def:230283	RHEL-08-010460 - There must be no shosts.equiv files on the RHEL 8 operating system.
oval:mil.disa.stig.rhel8os:def:230284	RHEL-08-010470 - There must be no .shosts files on the RHEL 8 operating system.
oval:mil.disa.stig.rhel8os:def:230286	RHEL-08-010480 - The RHEL 8 SSH public host key files must have mode 0644 or less permissive.
oval:mil.disa.stig.rhel8os:def:230287	RHEL-08-010490 - The RHEL 8 SSH private host key files must have mode 0640 or less permissive.
oval:mil.disa.stig.rhel8os:def:230288	RHEL-08-010500 - The RHEL 8 SSH daemon must perform strict mode checking of home directory configuration files.
oval:mil.disa.stig.rhel8os:def:230290	RHEL-08-010520 - The RHEL 8 SSH daemon must not allow authentication using known host’s authentication.
oval:mil.disa.stig.rhel8os:def:230291	RHEL-08-010521 - The RHEL 8 SSH daemon must not allow Kerberos authentication, except to fulfill documented and validated mission requirements.
oval:mil.disa.stig.rhel8os:def:230294	RHEL-08-010542 - RHEL 8 must use a separate file system for the system audit data path.
oval:mil.disa.stig.rhel8os:def:230295	RHEL-08-010543 - A separate RHEL 8 filesystem must be used for the /tmp directory.
oval:mil.disa.stig.rhel8os:def:230296	RHEL-08-010550 - RHEL 8 must not permit direct logons to the root account using remote access via SSH.
oval:mil.disa.stig.rhel8os:def:230299	RHEL-08-010570 - RHEL 8 must prevent files with the setuid and setgid bit set from being executed on file systems that contain user home directories.
oval:mil.disa.stig.rhel8os:def:230300	RHEL-08-010571 - RHEL 8 must prevent files with the setuid and setgid bit set from being executed on the /boot directory.
oval:mil.disa.stig.rhel8os:def:230301	RHEL-08-010580 - RHEL 8 must prevent special devices on non-root local partitions.
oval:mil.disa.stig.rhel8os:def:230306	RHEL-08-010630 - RHEL 8 must prevent code from being executed on file systems that are imported via Network File System (NFS).
oval:mil.disa.stig.rhel8os:def:230307	RHEL-08-010640 - RHEL 8 must prevent special devices on file systems that are imported via Network File System (NFS).
oval:mil.disa.stig.rhel8os:def:230308	RHEL-08-010650 - RHEL 8 must prevent files with the setuid and setgid bit set from being executed on file systems that are imported via Network File System (NFS).
oval:mil.disa.stig.rhel8os:def:230311	RHEL-08-010671 - RHEL 8 must disable the kernel.core_pattern.
oval:mil.disa.stig.rhel8os:def:230313	RHEL-08-010673 - RHEL 8 must disable core dumps for all users.
oval:mil.disa.stig.rhel8os:def:230314	RHEL-08-010674 - RHEL 8 must disable storing core dumps.
oval:mil.disa.stig.rhel8os:def:230315	RHEL-08-010675 - RHEL 8 must disable core dump backtraces.

Oval ID	Title
oval:mil.disa.stig.rhel8os:def:230320	RHEL-08-010720 - All RHEL 8 local interactive users must have a home directory assigned in the /etc/passwd file.
oval:mil.disa.stig.rhel8os:def:230321	RHEL-08-010730 - All RHEL 8 local interactive user home directories must have mode 0750 or less permissive.
oval:mil.disa.stig.rhel8os:def:230324	RHEL-08-010760 - All RHEL 8 local interactive user accounts must be assigned a home directory upon creation.
oval:mil.disa.stig.rhel8os:def:230325	RHEL-08-010770 - All RHEL 8 local initialization files must have mode 0740 or less permissive.
oval:mil.disa.stig.rhel8os:def:230328	RHEL-08-010800 - A separate RHEL 8 filesystem must be used for user home directories (such as /home or an equivalent).
oval:mil.disa.stig.rhel8os:def:230329	RHEL-08-010820 - Unattended or automatic logon via the RHEL 8 graphical user interface must not be allowed.
oval:mil.disa.stig.rhel8os:def:230330	RHEL-08-010830 - RHEL 8 must not allow users to override SSH environment variables.
oval:mil.disa.stig.rhel8os:def:230332	RHEL-08-020010 - RHEL 8 must automatically lock an account when three unsuccessful logon attempts occur.
oval:mil.disa.stig.rhel8os:def:230333	RHEL-08-020011 - RHEL 8 must automatically lock an account when three unsuccessful logon attempts occur.
oval:mil.disa.stig.rhel8os:def:230334	RHEL-08-020012 - RHEL 8 must automatically lock an account when three unsuccessful logon attempts occur during a 15-minute time period.
oval:mil.disa.stig.rhel8os:def:230335	RHEL-08-020013 - RHEL 8 must automatically lock an account when three unsuccessful logon attempts occur during a 15-minute time period.
oval:mil.disa.stig.rhel8os:def:230336	RHEL-08-020014 - RHEL 8 must automatically lock an account until the locked account is released by an administrator when three unsuccessful logon attempts occur during a 15-minute time period.
oval:mil.disa.stig.rhel8os:def:230337	RHEL-08-020015 - RHEL 8 must automatically lock an account until the locked account is released by an administrator when three unsuccessful logon attempts occur during a 15-minute time period.
oval:mil.disa.stig.rhel8os:def:230340	RHEL-08-020018 - RHEL 8 must prevent system messages from being presented when three unsuccessful logon attempts occur.
oval:mil.disa.stig.rhel8os:def:230341	RHEL-08-020019 - RHEL 8 must prevent system messages from being presented when three unsuccessful logon attempts occur.
oval:mil.disa.stig.rhel8os:def:230342	RHEL-08-020020 - RHEL 8 must log user name information when unsuccessful logon attempts occur.
oval:mil.disa.stig.rhel8os:def:230343	RHEL-08-020021 - RHEL 8 must log user name information when unsuccessful logon attempts occur.
oval:mil.disa.stig.rhel8os:def:230344	RHEL-08-020022 - RHEL 8 must include root when automatically locking an account until the locked account is released by an administrator when three unsuccessful logon attempts occur during a 15-minute time period.
oval:mil.disa.stig.rhel8os:def:230345	RHEL-08-020023 - RHEL 8 must include root when automatically locking an account until the locked account is released by an administrator when three unsuccessful logon attempts occur during a 15-minute time period.
oval:mil.disa.stig.rhel8os:def:230351	RHEL-08-020050 - RHEL 8 must be able to initiate directly a session lock for all connection types using smartcard when the smartcard is removed.
oval:mil.disa.stig.rhel8os:def:230354	RHEL-08-020080 - RHEL 8 must prevent a user from overriding the session lock-delay setting for the graphical user interface.

Oval ID	Title
oval:mil.disa.stig.rhel8os:def:230364	RHEL-08-020180 - RHEL 8 passwords must have a 24 hours/1 day minimum password lifetime restriction in /etc/shadow.
oval:mil.disa.stig.rhel8os:def:230365	RHEL-08-020190 - RHEL 8 passwords for new users or password changes must have a 24 hours/1 day minimum password lifetime restriction in /etc/login.defs.
oval:mil.disa.stig.rhel8os:def:230366	RHEL-08-020200 - RHEL 8 user account passwords must have a 60-day maximum password lifetime restriction.
oval:mil.disa.stig.rhel8os:def:230370	RHEL-08-020231 - RHEL 8 passwords for new users must have a minimum of 15 characters.
oval:mil.disa.stig.rhel8os:def:230373	RHEL-08-020260 - RHEL 8 account identifiers (individuals, groups, roles, and devices) must be disabled after 35 days of inactivity.
oval:mil.disa.stig.rhel8os:def:230377	RHEL-08-020300 - RHEL 8 must prevent the use of dictionary words for passwords.
oval:mil.disa.stig.rhel8os:def:230378	RHEL-08-020310 - RHEL 8 must enforce a delay of at least four seconds between logon prompts following a failed logon attempt.
oval:mil.disa.stig.rhel8os:def:230380	RHEL-08-020330 - RHEL 8 must not allow accounts configured with blank or null passwords.
oval:mil.disa.stig.rhel8os:def:230382	RHEL-08-020350 - RHEL 8 must display the date and time of the last successful account logon upon an SSH logon.
oval:mil.disa.stig.rhel8os:def:230383	RHEL-08-020351 - RHEL 8 must define default permissions for all authenticated users in such a way that the user can only read and modify their own files.
oval:mil.disa.stig.rhel8os:def:230386	RHEL-08-030000 - The RHEL 8 audit system must be configured to audit the execution of privileged functions and prevent all software from executing at higher privilege levels than users executing the software.
oval:mil.disa.stig.rhel8os:def:230388	RHEL-08-030020 - The RHEL 8 System Administrator (SA) and Information System Security Officer (ISSO) (at a minimum) must be alerted of an audit processing failure event.
oval:mil.disa.stig.rhel8os:def:230389	RHEL-08-030030 - The RHEL 8 Information System Security Officer (ISSO) and System Administrator (SA) (at a minimum) must have mail aliases to be notified of an audit processing failure.
oval:mil.disa.stig.rhel8os:def:230390	RHEL-08-030040 - The RHEL 8 System must take appropriate action when an audit processing failure occurs.
oval:mil.disa.stig.rhel8os:def:230392	RHEL-08-030060 - The RHEL 8 audit system must take appropriate action when the audit storage volume is full.
oval:mil.disa.stig.rhel8os:def:230393	RHEL-08-030061 - The RHEL 8 audit system must audit local events.
oval:mil.disa.stig.rhel8os:def:230394	RHEL-08-030062 - RHEL 8 must label all off-loaded audit logs before sending them to the central log server.
oval:mil.disa.stig.rhel8os:def:230395	RHEL-08-030063 - RHEL 8 must resolve audit information before writing to disk.
oval:mil.disa.stig.rhel8os:def:230397	RHEL-08-030080 - RHEL 8 audit logs must be owned by root to prevent unauthorized read access.
oval:mil.disa.stig.rhel8os:def:230398	RHEL-08-030090 - RHEL 8 audit logs must be group-owned by root to prevent unauthorized read access.
oval:mil.disa.stig.rhel8os:def:230399	RHEL-08-030100 - RHEL 8 audit log directory must be owned by root to prevent unauthorized read access.
oval:mil.disa.stig.rhel8os:def:230400	RHEL-08-030110 - RHEL 8 audit log directory must be group-owned by root to prevent unauthorized read access.

Oval ID	Title
oval:mil.disa.stig.rhel8os:def:230401	RHEL-08-030120 - RHEL 8 audit log directory must have a mode of 0700 or less permissive to prevent unauthorized read access.
oval:mil.disa.stig.rhel8os:def:230402	RHEL-08-030121 - RHEL 8 audit system must protect auditing rules from unauthorized change.
oval:mil.disa.stig.rhel8os:def:230403	RHEL-08-030122 - RHEL 8 audit system must protect logon UIDs from unauthorized change.
oval:mil.disa.stig.rhel8os:def:230404	RHEL-08-030130 - RHEL 8 must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/shadow.
oval:mil.disa.stig.rhel8os:def:230405	RHEL-08-030140 - RHEL 8 must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/security/opasswd.
oval:mil.disa.stig.rhel8os:def:230406	RHEL-08-030150 - RHEL 8 must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/passwd.
oval:mil.disa.stig.rhel8os:def:230407	RHEL-08-030160 - RHEL 8 must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/gshadow.
oval:mil.disa.stig.rhel8os:def:230408	RHEL-08-030170 - RHEL 8 must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/group.
oval:mil.disa.stig.rhel8os:def:230409	RHEL-08-030171 - RHEL 8 must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/sudoers.
oval:mil.disa.stig.rhel8os:def:230410	RHEL-08-030172 - RHEL 8 must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/sudoers.d/.
oval:mil.disa.stig.rhel8os:def:230411	RHEL-08-030180 - The RHEL 8 audit package must be installed.
oval:mil.disa.stig.rhel8os:def:230412	RHEL-08-030190 - Successful/unsuccessful uses of the su command in RHEL 8 must generate an audit record.
oval:mil.disa.stig.rhel8os:def:230413	RHEL-08-030200 - The RHEL 8 audit system must be configured to audit any usage of the setxattr, fsetxattr, lsetxattr, removexattr, fremovexattr, and lremovexattr system calls.
oval:mil.disa.stig.rhel8os:def:230418	RHEL-08-030250 - Successful/unsuccessful uses of the chage command in RHEL 8 must generate an audit record.
oval:mil.disa.stig.rhel8os:def:230419	RHEL-08-030260 - Successful/unsuccessful uses of the chcon command in RHEL 8 must generate an audit record.
oval:mil.disa.stig.rhel8os:def:230421	RHEL-08-030280 - Successful/unsuccessful uses of the ssh-agent in RHEL 8 must generate an audit record.
oval:mil.disa.stig.rhel8os:def:230422	RHEL-08-030290 - Successful/unsuccessful uses of the passwd command in RHEL 8 must generate an audit record.
oval:mil.disa.stig.rhel8os:def:230423	RHEL-08-030300 - Successful/unsuccessful uses of the mount command in RHEL 8 must generate an audit record.
oval:mil.disa.stig.rhel8os:def:230424	RHEL-08-030301 - Successful/unsuccessful uses of the umount command in RHEL 8 must generate an audit record.
oval:mil.disa.stig.rhel8os:def:230425	RHEL-08-030302 - Successful/unsuccessful uses of the mount syscall in RHEL 8 must generate an audit record.
oval:mil.disa.stig.rhel8os:def:230426	RHEL-08-030310 - Successful/unsuccessful uses of the unix_update in RHEL 8 must generate an audit record.
oval:mil.disa.stig.rhel8os:def:230427	RHEL-08-030311 - Successful/unsuccessful uses of postdrop in RHEL 8 must generate an audit record.

Oval ID	Title
oval:mil.disa.stig.rhel8os:def:230428	RHEL-08-030312 - Successful/unsuccessful uses of postqueue in RHEL 8 must generate an audit record.
oval:mil.disa.stig.rhel8os:def:230429	RHEL-08-030313 - Successful/unsuccessful uses of semanage in RHEL 8 must generate an audit record.
oval:mil.disa.stig.rhel8os:def:230430	RHEL-08-030314 - Successful/unsuccessful uses of setfiles in RHEL 8 must generate an audit record.
oval:mil.disa.stig.rhel8os:def:230431	RHEL-08-030315 - Successful/unsuccessful uses of userhelper in RHEL 8 must generate an audit record.
oval:mil.disa.stig.rhel8os:def:230432	RHEL-08-030316 - Successful/unsuccessful uses of setsebool in RHEL 8 must generate an audit record.
oval:mil.disa.stig.rhel8os:def:230433	RHEL-08-030317 - Successful/unsuccessful uses of unix_chkpwd in RHEL 8 must generate an audit record.
oval:mil.disa.stig.rhel8os:def:230434	RHEL-08-030320 - Successful/unsuccessful uses of the ssh-keysign in RHEL 8 must generate an audit record.
oval:mil.disa.stig.rhel8os:def:230435	RHEL-08-030330 - Successful/unsuccessful uses of the setfacl command in RHEL 8 must generate an audit record.
oval:mil.disa.stig.rhel8os:def:230436	RHEL-08-030340 - Successful/unsuccessful uses of the pam_timestamp_check command in RHEL 8 must generate an audit record.
oval:mil.disa.stig.rhel8os:def:230437	RHEL-08-030350 - Successful/unsuccessful uses of the newgrp command in RHEL 8 must generate an audit record.
oval:mil.disa.stig.rhel8os:def:230438	RHEL-08-030360 - Successful/unsuccessful uses of the init_module and finit_module system calls in RHEL 8 must generate an audit record.
oval:mil.disa.stig.rhel8os:def:230439	RHEL-08-030361 - Successful/unsuccessful uses of the rename, unlink, rmdir, renameat, and unlinkat system calls in RHEL 8 must generate an audit record.
oval:mil.disa.stig.rhel8os:def:230444	RHEL-08-030370 - Successful/unsuccessful uses of the gpasswd command in RHEL 8 must generate an audit record.
oval:mil.disa.stig.rhel8os:def:230446	RHEL-08-030390 - Successful/unsuccessful uses of the delete_module command in RHEL 8 must generate an audit record.
oval:mil.disa.stig.rhel8os:def:230447	RHEL-08-030400 - Successful/unsuccessful uses of the crontab command in RHEL 8 must generate an audit record.
oval:mil.disa.stig.rhel8os:def:230448	RHEL-08-030410 - Successful/unsuccessful uses of the chsh command in RHEL 8 must generate an audit record.
oval:mil.disa.stig.rhel8os:def:230449	RHEL-08-030420 - Successful/unsuccessful uses of the truncate, ftruncate, creat, open, openat, and open_by_handle_at system calls in RHEL 8 must generate an audit record.
oval:mil.disa.stig.rhel8os:def:230455	RHEL-08-030480 - Successful/unsuccessful uses of the chown, fchown, fchownat, and lchown system calls in RHEL 8 must generate an audit record.
oval:mil.disa.stig.rhel8os:def:230456	RHEL-08-030490 - Successful/unsuccessful uses of the chmod, fchmod, and fchmodat system calls in RHEL 8 must generate an audit record.
oval:mil.disa.stig.rhel8os:def:230462	RHEL-08-030550 - Successful/unsuccessful uses of the sudo command in RHEL 8 must generate an audit record.
oval:mil.disa.stig.rhel8os:def:230463	RHEL-08-030560 - Successful/unsuccessful uses of the usermod command in RHEL 8 must generate an audit record.
oval:mil.disa.stig.rhel8os:def:230464	RHEL-08-030570 - Successful/unsuccessful uses of the chacl command in RHEL 8 must generate an audit record.

Oval ID	Title
oval:mil.disa.stig.rhel8os:def:230465	RHEL-08-030580 - Successful/unsuccessful uses of the kmod command in RHEL 8 must generate an audit record.
oval:mil.disa.stig.rhel8os:def:230467	RHEL-08-030600 - Successful/unsuccessful modifications to the lastlog file in RHEL 8 must generate an audit record.
oval:mil.disa.stig.rhel8os:def:230471	RHEL-08-030610 - RHEL 8 must allow only the Information System Security Manager (ISSM) (or individuals or roles appointed by the ISSM) to select which auditable events are to be audited.
oval:mil.disa.stig.rhel8os:def:230472	RHEL-08-030620 - RHEL 8 audit tools must have a mode of 0755 or less permissive.
oval:mil.disa.stig.rhel8os:def:230473	RHEL-08-030630 - RHEL 8 audit tools must be owned by root.
oval:mil.disa.stig.rhel8os:def:230474	RHEL-08-030640 - RHEL 8 audit tools must be group-owned by root.
oval:mil.disa.stig.rhel8os:def:230477	RHEL-08-030670 - RHEL 8 must have the packages required for offloading audit logs installed.
oval:mil.disa.stig.rhel8os:def:230478	RHEL-08-030680 - RHEL 8 must have the packages required for encrypting offloaded audit logs installed.
oval:mil.disa.stig.rhel8os:def:230480	RHEL-08-030700 - RHEL 8 must take appropriate action when the internal event queue is full.
oval:mil.disa.stig.rhel8os:def:230482	RHEL-08-030720 - RHEL 8 must authenticate the remote logging server for off-loading audit logs.
oval:mil.disa.stig.rhel8os:def:230483	RHEL-08-030730 - RHEL 8 must take action when allocated audit record storage volume reaches 75 percent of the repository maximum audit record storage capacity.
oval:mil.disa.stig.rhel8os:def:230485	RHEL-08-030741 - RHEL 8 must disable the chrony daemon from acting as a server.
oval:mil.disa.stig.rhel8os:def:230486	RHEL-08-030742 - RHEL 8 must disable network management of the chrony daemon.
oval:mil.disa.stig.rhel8os:def:230487	RHEL-08-040000 - RHEL 8 must not have the telnet-server package installed.
oval:mil.disa.stig.rhel8os:def:230488	RHEL-08-040001 - RHEL 8 must not have any automated bug reporting tools installed.
oval:mil.disa.stig.rhel8os:def:230489	RHEL-08-040002 - RHEL 8 must not have the sendmail package installed.
oval:mil.disa.stig.rhel8os:def:230492	RHEL-08-040010 - RHEL 8 must not have the rsh-server package installed.
oval:mil.disa.stig.rhel8os:def:230505	RHEL-08-040100 - A firewall must be installed on RHEL 8.
oval:mil.disa.stig.rhel8os:def:230508	RHEL-08-040120 - RHEL 8 must mount /dev/shm with the nodev option.
oval:mil.disa.stig.rhel8os:def:230509	RHEL-08-040121 - RHEL 8 must mount /dev/shm with the nosuid option.
oval:mil.disa.stig.rhel8os:def:230510	RHEL-08-040122 - RHEL 8 must mount /dev/shm with the noexec option.
oval:mil.disa.stig.rhel8os:def:230511	RHEL-08-040123 - RHEL 8 must mount /tmp with the nodev option.
oval:mil.disa.stig.rhel8os:def:230512	RHEL-08-040124 - RHEL 8 must mount /tmp with the nosuid option.
oval:mil.disa.stig.rhel8os:def:230513	RHEL-08-040125 - RHEL 8 must mount /tmp with the noexec option.
oval:mil.disa.stig.rhel8os:def:230514	RHEL-08-040126 - RHEL 8 must mount /var/log with the nodev option.
oval:mil.disa.stig.rhel8os:def:230515	RHEL-08-040127 - RHEL 8 must mount /var/log with the nosuid option.
oval:mil.disa.stig.rhel8os:def:230516	RHEL-08-040128 - RHEL 8 must mount /var/log with the noexec option.

Oval ID	Title
oval:mil.disa.stig.rhel8os:def:230517	RHEL-08-040129 - RHEL 8 must mount /var/log/audit with the nodev option.
oval:mil.disa.stig.rhel8os:def:230518	RHEL-08-040130 - RHEL 8 must mount /var/log/audit with the nosuid option.
oval:mil.disa.stig.rhel8os:def:230519	RHEL-08-040131 - RHEL 8 must mount /var/log/audit with the noexec option.
oval:mil.disa.stig.rhel8os:def:230520	RHEL-08-040132 - RHEL 8 must mount /var/tmp with the nodev option.
oval:mil.disa.stig.rhel8os:def:230521	RHEL-08-040133 - RHEL 8 must mount /var/tmp with the nosuid option.
oval:mil.disa.stig.rhel8os:def:230522	RHEL-08-040134 - RHEL 8 must mount /var/tmp with the noexec option.
oval:mil.disa.stig.rhel8os:def:230523	RHEL-08-040135 - The RHEL 8 fapolicy module must be installed.
oval:mil.disa.stig.rhel8os:def:230525	RHEL-08-040150 - A firewall must be able to protect against or limit the effects of Denial of Service (DoS) attacks by ensuring RHEL 8 can implement rate-limiting measures on impacted network interfaces.
oval:mil.disa.stig.rhel8os:def:230526	RHEL-08-040160 - All RHEL 8 networked systems must have and implement SSH to protect the confidentiality and integrity of transmitted and received information, as well as information during preparation for transmission.
oval:mil.disa.stig.rhel8os:def:230527	RHEL-08-040161 - RHEL 8 must force a frequent session key renegotiation for SSH connections to the server.
oval:mil.disa.stig.rhel8os:def:230530	RHEL-08-040171 - The x86 Ctrl-Alt-Delete key sequence in RHEL 8 must be disabled if a graphical user interface is installed.
oval:mil.disa.stig.rhel8os:def:230531	RHEL-08-040172 - The systemd Ctrl-Alt-Delete burst key sequence in RHEL 8 must be disabled.
oval:mil.disa.stig.rhel8os:def:230533	RHEL-08-040190 - The Trivial File Transfer Protocol (TFTP) server package must not be installed if not required for RHEL 8 operational support.
oval:mil.disa.stig.rhel8os:def:230534	RHEL-08-040200 - The root account must be the only account having unrestricted access to the RHEL 8 system.
oval:mil.disa.stig.rhel8os:def:230535	RHEL-08-040210 - RHEL 8 must prevent IPv6 Internet Control Message Protocol (ICMP) redirect messages from being accepted.
oval:mil.disa.stig.rhel8os:def:230536	RHEL-08-040220 - RHEL 8 must not send Internet Control Message Protocol (ICMP) redirects.
oval:mil.disa.stig.rhel8os:def:230537	RHEL-08-040230 - RHEL 8 must not respond to Internet Control Message Protocol (ICMP) echoes sent to a broadcast address.
oval:mil.disa.stig.rhel8os:def:230538	RHEL-08-040240 - RHEL 8 must not forward IPv6 source-routed packets.
oval:mil.disa.stig.rhel8os:def:230539	RHEL-08-040250 - RHEL 8 must not forward IPv6 source-routed packets by default.
oval:mil.disa.stig.rhel8os:def:230540	RHEL-08-040260 - RHEL 8 must not enable IPv6 packet forwarding unless the system is a router.
oval:mil.disa.stig.rhel8os:def:230541	RHEL-08-040261 - RHEL 8 must not accept router advertisements on all IPv6 interfaces.
oval:mil.disa.stig.rhel8os:def:230542	RHEL-08-040262 - RHEL 8 must not accept router advertisements on all IPv6 interfaces by default.
oval:mil.disa.stig.rhel8os:def:230543	RHEL-08-040270 - RHEL 8 must not allow interfaces to perform Internet Control Message Protocol (ICMP) redirects by default.
oval:mil.disa.stig.rhel8os:def:230544	RHEL-08-040280 - RHEL 8 must ignore IPv6 Internet Control Message Protocol (ICMP) redirect messages.

Oval ID	Title
oval:mil.disa.stig.rhel8os:def:230545	RHEL-08-040281 - RHEL 8 must disable access to network bpf syscall from unprivileged processes.
oval:mil.disa.stig.rhel8os:def:230546	RHEL-08-040282 - RHEL 8 must restrict usage of ptrace to descendant processes.
oval:mil.disa.stig.rhel8os:def:230547	RHEL-08-040283 - RHEL 8 must restrict exposed kernel pointer addresses access.
oval:mil.disa.stig.rhel8os:def:230548	RHEL-08-040284 - RHEL 8 must disable the use of user namespaces.
oval:mil.disa.stig.rhel8os:def:230549	RHEL-08-040285 - RHEL 8 must use reverse path filtering on all IPv4 interfaces.
oval:mil.disa.stig.rhel8os:def:230550	RHEL-08-040290 - RHEL 8 must be configured to prevent unrestricted mail relaying.
oval:mil.disa.stig.rhel8os:def:230553	RHEL-08-040320 - The graphical display manager must not be installed on RHEL 8 unless approved.
oval:mil.disa.stig.rhel8os:def:230554	RHEL-08-040330 - RHEL 8 network interfaces must not be in promiscuous mode.
oval:mil.disa.stig.rhel8os:def:230555	RHEL-08-040340 - RHEL 8 remote X connections for interactive users must be disabled unless to fulfill documented and validated mission requirements.
oval:mil.disa.stig.rhel8os:def:230556	RHEL-08-040341 - The RHEL 8 SSH daemon must prevent remote hosts from connecting to the proxy display.
oval:mil.disa.stig.rhel8os:def:230557	RHEL-08-040350 - If the Trivial File Transfer Protocol (TFTP) server is required, the RHEL 8 TFTP daemon must be configured to operate in secure mode.
oval:mil.disa.stig.rhel8os:def:230558	RHEL-08-040360 - A File Transfer Protocol (FTP) server package must not be installed unless mission essential on RHEL 8.
oval:mil.disa.stig.rhel8os:def:230560	RHEL-08-040380 - The iprutils package must not be installed unless mission essential on RHEL 8.
oval:mil.disa.stig.rhel8os:def:230561	RHEL-08-040390 - The tuned package must not be installed unless mission essential on RHEL 8.
oval:mil.disa.stig.rhel8os:def:237640	RHEL-08-010163 - The krb5-server package must not be installed on RHEL 8.
oval:mil.disa.stig.rhel8os:def:237641	RHEL-08-010382 - RHEL 8 must restrict privilege elevation to authorized personnel.
oval:mil.disa.stig.rhel8os:def:237642	RHEL-08-010383 - RHEL 8 must use the invoking user's password for privilege escalation when using "sudo".
oval:mil.disa.stig.rhel8os:def:237643	RHEL-08-010384 - RHEL 8 must require re-authentication when using the "sudo" command.
oval:mil.disa.stig.rhel8os:def:244519	RHEL-08-010049 - RHEL 8 must display a banner before granting local or remote access to the system via a graphical user logon.
oval:mil.disa.stig.rhel8os:def:244523	RHEL-08-010152 - RHEL 8 operating systems must require authentication upon booting into emergency mode.
oval:mil.disa.stig.rhel8os:def:244525	RHEL-08-010201 - The RHEL 8 SSH daemon must be configured with a timeout interval.
oval:mil.disa.stig.rhel8os:def:244527	RHEL-08-010472 - RHEL 8 must have the packages required to use the hardware random number generator entropy gatherer service.
oval:mil.disa.stig.rhel8os:def:244528	RHEL-08-010522 - The RHEL 8 SSH daemon must not allow GSSAPI authentication, except to fulfill documented and validated mission requirements.
oval:mil.disa.stig.rhel8os:def:244529	RHEL-08-010544 - RHEL 8 must use a separate file system for /var/tmp.

Oval ID	Title
oval:mil.disa.stig.rhel8os:def:244530	RHEL-08-010572 - RHEL 8 must prevent files with the setuid and setgid bit set from being executed on the /boot/efi directory.
oval:mil.disa.stig.rhel8os:def:244536	RHEL-08-020032 - RHEL 8 must disable the user list at logon for graphical user interfaces.
oval:mil.disa.stig.rhel8os:def:244539	RHEL-08-020082 - RHEL 8 must prevent a user from overriding the screensaver lock-enabled setting for the graphical user interface.
oval:mil.disa.stig.rhel8os:def:244541	RHEL-08-020332 - RHEL 8 must not allow blank or null passwords in the password-auth file.
oval:mil.disa.stig.rhel8os:def:244543	RHEL-08-030731 - RHEL 8 must notify the System Administrator (SA) and Information System Security Officer (ISSO) (at a minimum) when allocated audit record storage volume 75 percent utilization.
oval:mil.disa.stig.rhel8os:def:244547	RHEL-08-040139 - RHEL 8 must have the USBGuard installed.
oval:mil.disa.stig.rhel8os:def:244549	RHEL-08-040159 - All RHEL 8 networked systems must have SSH installed.
oval:mil.disa.stig.rhel8os:def:244550	RHEL-08-040209 - RHEL 8 must prevent IPv4 Internet Control Message Protocol (ICMP) redirect messages from being accepted.
oval:mil.disa.stig.rhel8os:def:244551	RHEL-08-040239 - RHEL 8 must not forward IPv4 source-routed packets.
oval:mil.disa.stig.rhel8os:def:244552	RHEL-08-040249 - RHEL 8 must not forward IPv4 source-routed packets by default.
oval:mil.disa.stig.rhel8os:def:244553	RHEL-08-040279 - RHEL 8 must ignore IPv4 Internet Control Message Protocol (ICMP) redirect messages.
oval:mil.disa.stig.rhel8os:def:244554	RHEL-08-040286 - RHEL 8 must enable hardening for the Berkeley Packet Filter Just-in-time compiler.
oval:mil.disa.stig.rhel8os:def:251706	RHEL-08-010121 - The RHEL 8 operating system must not have accounts configured with blank or null passwords.
oval:mil.disa.stig.rhel8os:def:251707	RHEL-08-010331 - RHEL 8 library directories must have mode 755 or less permissive.
oval:mil.disa.stig.rhel8os:def:251708	RHEL-08-010341 - RHEL 8 library directories must be owned by root.
oval:mil.disa.stig.rhel8os:def:251709	RHEL-08-010351 - RHEL 8 library directories must be group-owned by root or a system account.
oval:mil.disa.stig.rhel8os:def:251712	RHEL-08-010385 - The RHEL 8 operating system must not be configured to bypass password requirements for privilege escalation.
oval:mil.disa.stig.rhel8os:def:251713	RHEL-08-020101 - RHEL 8 must ensure the password complexity module is enabled in the system-auth file.
oval:mil.disa.stig.windows10:def:220860	WN10-CC-000326 - PowerShell script block logging must be enabled on Windows 10.
oval:mil.disa.stig.windows2019:def:205639	WN19-CC-000460 - Windows Server 2019 PowerShell script block logging must be enabled.
oval:mil.disa.stig.windows10:def:220777	WN10-AU-000155 - The system must be configured to audit System - System Integrity failures.
oval:mil.disa.stig.windows10:def:220801	WN10-CC-000039 - Run as different user must be removed from context menus.
oval:mil.disa.stig.windows2019:def:205871	WN19-CC-000320 - Windows Server 2019 Turning off File Explorer heap termination on corruption must be disabled.
oval:mil.disa.stig.windows2019:def:205824	WN19-SO-000110 - Windows Server 2019 must be configured to require a strong session key.

Oval ID	Title
oval:mil.disa.stig.windows10:def:220697	WN10-00-000005 - Domain-joined systems must use Windows 10 Enterprise Edition 64-bit version.
oval:mil.disa.stig.windows10:def:220847	WN10-CC-000260 - Windows 10 must be configured to require a minimum pin length of six characters or greater.
oval:mil.disa.stig.windows2019:def:205836	WN19-AU-000220 - Windows Server 2019 must be configured to audit Object Access - Other Object Access Events successes.
oval:mil.disa.stig.windows10:def:220746	WN10-AC-000040 - The built-in Microsoft password complexity filter must be enabled.
oval:mil.disa.stig.windows10:def:220850	WN10-CC-000280 - Remote Desktop Services must always prompt a client for passwords upon connection.
oval:mil.disa.stig.windows10:def:220908	WN10-SO-000005 - The built-in administrator account must be disabled.
oval:mil.disa.stig.windows2019:def:205702	WN19-DC-000020 - Windows Server 2019 Kerberos user logon restrictions must be enforced.
oval:mil.disa.stig.windows10:def:220727	WN10-00-000150 - Structured Exception Handling Overwrite Protection (SEHOP) must be enabled.
oval:mil.disa.stig.windows2019:def:205708	WN19-SO-000290 - Windows Server 2019 Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.
oval:mil.disa.stig.windows10:def:220942	WN10-SO-000230 - The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.
oval:mil.disa.stig.windows10:def:220914	WN10-SO-000035 - Outgoing secure channel traffic must be encrypted or signed.
oval:mil.disa.stig.windows2019:def:205816	WN19-CC-000480 - Windows Server 2019 Windows Remote Management (WinRM) client must not allow unencrypted traffic.
oval:mil.disa.stig.windows10:def:220757	WN10-AU-000065 - The system must be configured to audit Logon/Logoff - Logoff successes.
oval:mil.disa.stig.windows10:def:220833	WN10-CC-000204 - If Enhanced diagnostic data is enabled it must be limited to the minimum required to support Windows Analytics.
oval:mil.disa.stig.defs:def:253392	Enhanced diagnostic data must be limited to the minimum required to support Windows Analytics.
oval:mil.disa.stig.windows10:def:220909	WN10-SO-000010 - The built-in guest account must be disabled.
oval:mil.disa.stig.windows2019:def:205656	WN19-AC-000060 - Windows Server 2019 minimum password age must be configured to at least one day.
oval:mil.disa.stig.windows2019:def:205692	WN19-CC-000300 - Windows Server 2019 Windows Defender SmartScreen must be enabled.
oval:mil.disa.stig.windows10:def:220940	WN10-SO-000215 - The system must be configured to meet the minimum session security requirement for NTLM SSP based clients.
oval:mil.disa.stig.windows10:def:220790	WN10-AU-000575 - Windows 10 must be configured to audit MPSSVC Rule-Level Policy Change Successes.
oval:mil.disa.stig.windows10:def:220935	WN10-SO-000185 - PKU2U authentication using online identities must be prevented.
oval:mil.disa.stig.windows10:def:220778	WN10-AU-000160 - The system must be configured to audit System - System Integrity successes.
oval:mil.disa.stig.windows10:def:220840	WN10-CC-000230 - Users must not be allowed to ignore Windows Defender SmartScreen filter warnings for malicious websites in Microsoft Edge.

Oval ID	Title
oval:mil.disa.stig.defs:def:220840	Users must not be allowed to ignore Windows Defender SmartScreen filter warnings for malicious websites in Microsoft Edge.
oval:mil.disa.stig.windows10:def:220869	WN10-CC-000365 - Windows 10 must be configured to prevent Windows apps from being activated by voice while the system is locked.
oval:mil.disa.stig.windows2019:def:205630	WN19-AC-000030 - Windows Server 2019 must have the period of time before the bad logon counter is reset configured to 15 minutes or greater.
oval:mil.disa.stig.windows2019:def:205873	WN19-CC-000390 - Windows Server 2019 must prevent attachments from being downloaded from RSS feeds.
oval:mil.disa.stig.windows10:def:220852	WN10-CC-000290 - Remote Desktop Services must be configured with the client connection encryption set to the required level.
oval:mil.disa.stig.windows10:def:220794	WN10-CC-000010 - The display of slide shows on the lock screen must be disabled.
oval:mil.disa.stig.windows10:def:220729	WN10-00-000160 - The Server Message Block (SMB) v1 protocol must be disabled on the system.
oval:mil.disa.stig.windows10:def:220788	WN10-AU-000565 - Windows 10 must be configured to audit other Logon/Logoff Events Failures.
oval:mil.disa.stig.windows2019:def:205859	WN19-CC-000040 - Windows Server 2019 source routing must be configured to the highest protection level to prevent Internet Protocol (IP) source routing.
oval:mil.disa.stig.windows10:def:220744	WN10-AC-000030 - The minimum password age must be configured to at least 1 day.
oval:mil.disa.stig.windows2019:def:205711	WN19-CC-000470 - Windows Server 2019 Windows Remote Management (WinRM) client must not use Basic authentication.
oval:mil.disa.stig.windows10:def:220774	WN10-AU-000135 - The system must be configured to audit System - Other System Events failures.
oval:mil.disa.stig.windows10:def:220740	WN10-AC-000010 - The number of allowed bad logon attempts must be configured to 3 or less.
oval:mil.disa.stig.windows10:def:220770	WN10-AU-000110 - The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.
oval:mil.disa.stig.windows10:def:220828	WN10-CC-000185 - The default autorun behavior must be configured to prevent autorun commands.
oval:mil.disa.stig.windows2019:def:205920	WN19-SO-000320 - Windows Server 2019 must be configured to at least negotiate signing for LDAP client signing.
oval:mil.disa.stig.windows2019:def:205792	WN19-DC-000250 - Windows Server 2019 must be configured to audit DS Access - Directory Service Access failures.
oval:mil.disa.stig.windows10:def:220918	WN10-SO-000055 - The maximum age for machine account passwords must be configured to 30 days or less.
oval:mil.disa.stig.windows10:def:220919	WN10-SO-000060 - The system must be configured to require a strong session key.
oval:mil.disa.stig.windows2019:def:205860	WN19-CC-000050 - Windows Server 2019 must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF)-generated routes.
oval:mil.disa.stig.windows2019:def:205637	WN19-CC-000380 - Windows Server 2019 Remote Desktop Services must be configured with the client connection encryption set to High Level.
oval:mil.disa.stig.windows10:def:220819	WN10-CC-000120 - The network selection user interface (UI) must not be displayed on the logon screen.

Oval ID	Title
oval:mil.disa.stig.windows2019:def:205810	WN19-CC-000520 - Windows Server 2019 Windows Remote Management (WinRM) service must not store RunAs credentials.
oval:mil.disa.stig.windows2019:def:205725	WN19-SO-000250 - Windows Server 2019 must restrict anonymous access to Named Pipes and Shares.
oval:mil.disa.stig.windows2019:def:205773	WN19-AU-000280 - Windows Server 2019 must be configured to audit Policy Change - Authentication Policy Change successes.
oval:mil.disa.stig.windows10:def:220911	WN10-SO-000020 - The built-in administrator account must be renamed.
oval:mil.disa.stig.windows10:def:220862	WN10-CC-000330 - The Windows Remote Management (WinRM) client must not use Basic authentication.
oval:mil.disa.stig.windows10:def:220826	WN10-CC-000175 - The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.
oval:mil.disa.stig.windows2019:def:205687	WN19-CC-000020 - Windows Server 2019 must have WDigest Authentication disabled.
oval:mil.disa.stig.windows2019:def:205833	WN19-AU-000080 - Windows Server 2019 must be configured to audit Account Logon - Credential Validation failures.
oval:mil.disa.stig.windows2019:def:205717	WN19-SO-000400 - Windows Server 2019 User Account Control must, at a minimum, prompt administrators for consent on the secure desktop.
oval:mil.disa.stig.windows2019:def:205832	WN19-AU-000070 - Windows Server 2019 must be configured to audit Account Logon - Credential Validation successes.
oval:mil.disa.stig.windows10:def:220915	WN10-SO-000040 - Outgoing secure channel traffic must be encrypted when possible.
oval:mil.disa.stig.windows10:def:220841	WN10-CC-000235 - Users must not be allowed to ignore Windows Defender SmartScreen filter warnings for unverified files in Microsoft Edge.
oval:mil.disa.stig.defs:def:220841	Users must not be allowed to ignore Windows Defender SmartScreen filter warnings for unverified files in Microsoft Edge.
oval:mil.disa.stig.windows10:def:220949	WN10-SO-000265 - User Account Control must only elevate UIAccess applications that are installed in secure locations.
oval:mil.disa.stig.windows2019:def:205820	WN19-DC-000320 - Windows Server 2019 domain controllers must require LDAP access signing.
oval:mil.disa.stig.windows10:def:220863	WN10-CC-000335 - The Windows Remote Management (WinRM) client must not allow unencrypted traffic.
oval:mil.disa.stig.windows10:def:220760	WN10-AU-000080 - The system must be configured to audit Logon/Logoff - Special Logon successes.
oval:mil.disa.stig.windows10:def:220813	WN10-CC-000085 - Early Launch Antimalware, Boot-Start Driver Initialization Policy must prevent boot drivers.
oval:mil.disa.stig.windows10:def:220752	WN10-AU-000040 - The system must be configured to audit Account Management - User Account Management successes.
oval:mil.disa.stig.windows2019:def:205814	WN19-MS-000040 - Windows Server 2019 must restrict unauthenticated Remote Procedure Call (RPC) clients from connecting to the RPC server on domain-joined member servers and standalone or nondomain-joined systems.
oval:mil.disa.stig.windows2019:def:205660	WN19-AC-000040 - Windows Server 2019 password history must be configured to 24 passwords remembered.
oval:mil.disa.stig.windows10:def:220775	WN10-AU-000140 - The system must be configured to audit System - Security State Change successes.

Oval ID	Title
oval:mil.disa.stig.windows2019:def:205914	WN19-SO-000220 - Windows Server 2019 must not allow anonymous enumeration of Security Account Manager (SAM) accounts.
oval:mil.disa.stig.windows10:def:220818	WN10-CC-000115 - Systems must at least attempt device authentication using certificates.
oval:mil.disa.stig.windows2019:def:205655	WN19-SO-000180 - Windows Server 2019 unencrypted passwords must not be sent to third-party Server Message Block (SMB) servers.
oval:mil.disa.stig.windows2019:def:205910	WN19-SO-000040 - Windows Server 2019 built-in guest account must be renamed.
oval:mil.disa.stig.windows10:def:220762	WN10-AU-000082 - Windows 10 must be configured to audit Object Access - File Share successes.
oval:mil.disa.stig.windows2019:def:205830	WN19-CC-000310 - Windows Server 2019 Explorer Data Execution Prevention must be enabled.
oval:mil.disa.stig.windows10:def:220865	WN10-CC-000345 - The Windows Remote Management (WinRM) service must not use Basic authentication.
oval:mil.disa.stig.windows10:def:220931	WN10-SO-000160 - The system must be configured to prevent anonymous users from having the same rights as the Everyone group.
oval:mil.disa.stig.windows2019:def:205681	WN19-00-000370 - Windows Server 2019 must not have the TFTP Client installed.
oval:mil.disa.stig.windows2019:def:205916	WN19-SO-000260 - Windows Server 2019 services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity instead of authenticating anonymously.
oval:mil.disa.stig.windows10:def:220728	WN10-00-000155 - The Windows PowerShell 2.0 feature must be disabled on the system.
oval:mil.disa.stig.windows10:def:220842	WN10-CC-000238 - Windows 10 must be configured to prevent certificate error overrides in Microsoft Edge.
oval:mil.disa.stig.defs:def:220842	Windows must be configured to prevent certificate error overrides in Microsoft Edge.
oval:mil.disa.stig.windows10:def:220716	WN10-00-000090 - Accounts must be configured to require password expiration.
oval:mil.disa.stig.defs:def:253273	Accounts must be configured to require password expiration.
oval:mil.disa.stig.windows10:def:220830	WN10-CC-000195 - Enhanced anti-spoofing for facial recognition must be enabled on Window 10.
oval:mil.disa.stig.windows10:def:220708	WN10-00-000050 - Local volumes must be formatted using NTFS.
oval:mil.disa.stig.windows2019:def:205822	WN19-SO-000070 - Windows Server 2019 setting Domain member: Digitally encrypt secure channel data (when possible) must be configured to enabled.
oval:mil.disa.stig.windows10:def:220941	WN10-SO-000220 - The system must be configured to meet the minimum session security requirement for NTLM SSP based servers.
oval:mil.disa.stig.windows10:def:220720	WN10-00-000110 - Simple TCP/IP Services must not be installed on the system.
oval:mil.disa.stig.windows2019:def:205923	WN19-SO-000370 - Windows Server 2019 default permissions of global system objects must be strengthened.
oval:mil.disa.stig.windows10:def:220829	WN10-CC-000190 - Autoplay must be disabled for all drives.
oval:mil.disa.stig.windows10:def:220722	WN10-00-000120 - The TFTP Client must not be installed on the system.
oval:mil.disa.stig.windows2019:def:205811	WN19-SO-000380 - Windows Server 2019 User Account Control approval mode for the built-in Administrator must be enabled.

Oval ID	Title
oval:mil.disa.stig.windows2019:def:205629	WN19-AC-000020 - Windows Server 2019 must have the number of allowed bad logon attempts configured to three or less.
oval:mil.disa.stig.windows2019:def:205771	WN19-AU-000260 - Windows Server 2019 must be configured to audit Policy Change - Audit Policy Change successes.
oval:mil.disa.stig.windows2019:def:205689	WN19-CC-000160 - Windows Server 2019 printing over HTTP must be turned off.
oval:mil.disa.stig.windows10:def:220789	WN10-AU-000570 - Windows 10 must be configured to audit Detailed File Share Failures.
oval:mil.disa.stig.windows2019:def:205867	WN19-CC-000180 - Windows Server 2019 users must be prompted to authenticate when the system wakes from sleep (on battery).
oval:mil.disa.stig.windows10:def:220798	WN10-CC-000035 - The system must be configured to ignore NetBIOS name release requests except from WINS servers.
oval:mil.disa.stig.windows10:def:220802	WN10-CC-000040 - Insecure logons to an SMB server must be disabled.
oval:mil.disa.stig.windows10:def:220910	WN10-SO-000015 - Local accounts with blank passwords must be restricted to prevent access from the network.
oval:mil.disa.stig.windows2019:def:205842	WN19-SO-000360 - Windows Server 2019 must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.
oval:mil.disa.stig.windows2019:def:205925	WN19-CC-000450 - Windows Server 2019 must disable automatically signing in the last interactive user after a system-initiated restart.
oval:mil.disa.stig.windows10:def:220917	WN10-SO-000050 - The computer account password must not be prevented from being reset.
oval:mil.disa.stig.windows10:def:220932	WN10-SO-000165 - Anonymous access to Named Pipes and Shares must be restricted.
oval:mil.disa.stig.windows2019:def:205688	WN19-CC-000150 - Windows Server 2019 downloading print driver packages over HTTP must be turned off.
oval:mil.disa.stig.windows2019:def:205917	WN19-SO-000270 - Windows Server 2019 must prevent NTLM from falling back to a Null session.
oval:mil.disa.stig.windows2019:def:205806	WN19-CC-000230 - Windows Server 2019 AutoPlay must be disabled for all drives.
oval:mil.disa.stig.windows2019:def:205678	WN19-00-000320 - Windows Server 2019 must not have the Fax Server role installed.
oval:mil.disa.stig.windows2019:def:205712	WN19-CC-000490 - Windows Server 2019 Windows Remote Management (WinRM) client must not use Digest authentication.
oval:mil.disa.stig.windows10:def:220948	WN10-SO-000260 - User Account Control must be configured to detect application installations and prompt for elevation.
oval:mil.disa.stig.windows10:def:220799	WN10-CC-000037 - Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.
oval:mil.disa.stig.windows10:def:220843	WN10-CC-000245 - The password manager function in the Edge browser must be disabled.
oval:mil.disa.stig.defs:def:220843	The password manager function in the Edge browser must be disabled.
oval:mil.disa.stig.windows2019:def:205634	WN19-AU-000190 - Windows Server 2019 must be configured to audit logon successes.
oval:mil.disa.stig.windows2019:def:205865	WN19-CC-000130 - Windows Server 2019 Early Launch Antimalware, Boot-Start Driver Initialization Policy must prevent boot drivers identified as bad.

Oval ID	Title
oval:mil.disa.stig.windows10:def:220836	WN10-CC-000210 - The Windows Defender SmartScreen for Explorer must be enabled.
oval:mil.disa.stig.windows10:def:220703	WN10-00-000031 - Windows 10 systems must use a BitLocker PIN for pre-boot authentication.
oval:mil.disa.stig.windows2019:def:205652	WN19-AC-000080 - Windows Server 2019 must have the built-in Windows password complexity policy enabled.
oval:mil.disa.stig.windows10:def:220776	WN10-AU-000150 - The system must be configured to audit System - Security System Extension successes.
oval:mil.disa.stig.windows10:def:220768	WN10-AU-000105 - The system must be configured to audit Policy Change - Authentication Policy Change successes.
oval:mil.disa.stig.windows2019:def:205861	WN19-CC-000070 - Windows Server 2019 insecure logons to an SMB server must be disabled.
oval:mil.disa.stig.windows2019:def:205821	WN19-SO-000060 - Windows Server 2019 setting Domain member: Digitally encrypt or sign secure channel data (always) must be configured to Enabled.
oval:mil.disa.stig.windows10:def:220786	WN10-AU-000555 - Windows 10 must be configured to audit Other Policy Change Events Failures.
oval:mil.disa.stig.windows2019:def:205784	WN19-AU-000390 - Windows Server 2019 must be configured to audit System - System Integrity failures.
oval:mil.disa.stig.windows10:def:220755	WN10-AU-000054 - The system must be configured to audit Logon/Logoff - Account Lockout failures.
oval:mil.disa.stig.windows2019:def:205720	WN19-SO-000450 - Windows Server 2019 User Account Control (UAC) must virtualize file and registry write failures to per-user locations.
oval:mil.disa.stig.windows10:def:220832	WN10-CC-000200 - Administrator accounts must not be enumerated during elevation.
oval:mil.disa.stig.windows10:def:220947	WN10-SO-000255 - User Account Control must automatically deny elevation requests for standard users.
oval:mil.disa.stig.windows2019:def:205713	WN19-CC-000500 - Windows Server 2019 Windows Remote Management (WinRM) service must not use Basic authentication.
oval:mil.disa.stig.windows10:def:220944	WN10-SO-000245 - User Account Control approval mode for the built-in Administrator must be enabled.
oval:mil.disa.stig.windows10:def:220913	WN10-SO-000030 - Audit policy using subcategories must be enabled.
oval:mil.disa.stig.windows2019:def:205772	WN19-AU-000270 - Windows Server 2019 must be configured to audit Policy Change - Audit Policy Change failures.
oval:mil.disa.stig.windows10:def:220771	WN10-AU-000115 - The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.
oval:mil.disa.stig.windows2019:def:205770	WN19-AU-000140 - Windows Server 2019 must be configured to audit Detailed Tracking - Process Creation successes.
oval:mil.disa.stig.windows10:def:220773	WN10-AU-000130 - The system must be configured to audit System - Other System Events successes.
oval:mil.disa.stig.windows2019:def:205828	WN19-SO-000200 - Windows Server 2019 setting Microsoft network server: Digitally sign communications (if client agrees) must be configured to Enabled.
oval:mil.disa.stig.windows2019:def:205866	WN19-CC-000140 - Windows Server 2019 group policy objects must be reprocessed even if they have not changed.
oval:mil.disa.stig.windows10:def:220916	WN10-SO-000045 - Outgoing secure channel traffic must be signed when possible.

Oval ID	Title
oval:mil.disa.stig.windows2019:def:205686	WN19-CC-000010 - Windows Server 2019 must prevent the display of slide shows on the lock screen.
oval:mil.disa.stig.windows2019:def:205690	WN19-CC-000170 - Windows Server 2019 network selection user interface (UI) must not be displayed on the logon screen.
oval:mil.disa.stig.windows10:def:220779	WN10-AU-000500 - The Application event log size must be configured to 32768 KB or greater.
oval:mil.disa.stig.windows2019:def:205827	WN19-SO-000190 - Windows Server 2019 setting Microsoft network server: Digitally sign communications (always) must be configured to Enabled.
oval:mil.disa.stig.windows2019:def:205635	WN19-AU-000200 - Windows Server 2019 must be configured to audit logon failures.
oval:mil.disa.stig.windows10:def:220867	WN10-CC-000355 - The Windows Remote Management (WinRM) service must not store RunAs credentials.
oval:mil.disa.stig.windows10:def:220742	WN10-AC-000020 - The password history must be configured to 24 passwords remembered.
oval:mil.disa.stig.windows2019:def:205815	WN19-SO-000090 - Windows Server 2019 computer account password must not be prevented from being reset.
oval:mil.disa.stig.windows10:def:220795	WN10-CC-000020 - IPv6 source routing must be configured to highest protection.
oval:mil.disa.stig.windows10:def:220936	WN10-SO-000190 - Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.
oval:mil.disa.stig.windows2019:def:205922	WN19-SO-000340 - Windows Server 2019 session security for NTLM SSP-based servers must be configured to require NTLMv2 session security and 128-bit encryption.
oval:mil.disa.stig.windows2019:def:205797	WN19-CC-000280 - Windows Server 2019 Security event log size must be configured to 196608 KB or greater.
oval:mil.disa.stig.windows2019:def:205777	WN19-AU-000320 - Windows Server 2019 must be configured to audit System - IPsec Driver successes.
oval:mil.disa.stig.windows2019:def:205793	WN19-DC-000260 - Windows Server 2019 must be configured to audit DS Access - Directory Service Changes successes.
oval:mil.disa.stig.windows2019:def:205796	WN19-CC-000270 - Windows Server 2019 Application event log size must be configured to 32768 KB or greater.
oval:mil.disa.stig.windows2019:def:205838	WN19-AU-000180 - Windows Server 2019 must be configured to audit logoff successes.
oval:mil.disa.stig.windows10:def:220761	WN10-AU-000081 - Windows 10 must be configured to audit Object Access - File Share failures.
oval:mil.disa.stig.windows10:def:220851	WN10-CC-000285 - The Remote Desktop Session Host must require secure RPC communications.
oval:mil.disa.stig.windows2019:def:205780	WN19-AU-000350 - Windows Server 2019 must be configured to audit System - Other System Events failures.
oval:mil.disa.stig.windows2019:def:205825	WN19-SO-000160 - Windows Server 2019 setting Microsoft network client: Digitally sign communications (always) must be configured to Enabled.
oval:mil.disa.stig.windows2019:def:205783	WN19-AU-000380 - Windows Server 2019 must be configured to audit System - System Integrity successes.
oval:mil.disa.stig.windows2019:def:205704	WN19-DC-000040 - Windows Server 2019 Kerberos user ticket lifetime must be limited to 10 hours or less.

Oval ID	Title
oval:mil.disa.stig.windows2019:def:205644	WN19-SO-000050 - Windows Server 2019 must force audit policy subcategory settings to override audit policy category settings.
oval:mil.disa.stig.windows2019:def:205626	WN19-AU-000110 - Windows Server 2019 must be configured to audit Account Management - User Account Management successes.
oval:mil.disa.stig.windows10:def:220937	WN10-SO-000195 - The system must be configured to prevent the storage of the LAN Manager hash of passwords.
oval:mil.disa.stig.windows2019:def:205718	WN19-SO-000420 - Windows Server 2019 User Account Control must be configured to detect application installations and prompt for elevation.
oval:mil.disa.stig.windows10:def:220857	WN10-CC-000315 - The Windows Installer Always install with elevated privileges must be disabled.
oval:mil.disa.stig.windows10:def:220796	WN10-CC-000025 - The system must be configured to prevent IP source routing.
oval:mil.disa.stig.windows2019:def:205716	WN19-SO-000390 - Windows Server 2019 UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.
oval:mil.disa.stig.windows10:def:220751	WN10-AU-000035 - The system must be configured to audit Account Management - User Account Management failures.
oval:mil.disa.stig.windows10:def:220846	WN10-CC-000255 - The use of a hardware security device with Windows Hello for Business must be enabled.
oval:mil.disa.stig.windows2019:def:205870	WN19-CC-000260 - Windows Server 2019 Windows Update must not obtain updates from other PCs on the Internet.
oval:mil.disa.stig.windows2019:def:205778	WN19-AU-000330 - Windows Server 2019 must be configured to audit System - IPsec Driver failures.
oval:mil.disa.stig.windows2019:def:205693	WN19-CC-000400 - Windows Server 2019 must disable Basic authentication for RSS feeds over HTTP.
oval:mil.disa.stig.windows10:def:220807	WN10-CC-000060 - Connections to non-domain networks when connected to a domain authenticated network must be blocked.
oval:mil.disa.stig.windows2019:def:205706	WN19-DC-000060 - Windows Server 2019 computer clock synchronization tolerance must be limited to five minutes or less.
oval:mil.disa.stig.windows10:def:220912	WN10-SO-000025 - The built-in guest account must be renamed.
oval:mil.disa.stig.windows2019:def:205798	WN19-CC-000290 - Windows Server 2019 System event log size must be configured to 32768 KB or greater.
oval:mil.disa.stig.windows2019:def:205654	WN19-SO-000300 - Windows Server 2019 must be configured to prevent the storage of the LAN Manager hash of passwords.
oval:mil.disa.stig.windows2019:def:205781	WN19-AU-000360 - Windows Server 2019 must be configured to audit System - Security State Change successes.
oval:mil.disa.stig.windows10:def:220747	WN10-AC-000045 - Reversible password encryption must be disabled.
oval:mil.disa.stig.windows2019:def:205694	WN19-CC-000410 - Windows Server 2019 must prevent Indexing of encrypted files.
oval:mil.disa.stig.windows10:def:220815	WN10-CC-000100 - Downloading print driver packages over HTTP must be prevented.
oval:mil.disa.stig.windows10:def:220822	WN10-CC-000150 - The user must be prompted for a password on resume from sleep (plugged in).
oval:mil.disa.stig.windows10:def:220950	WN10-SO-000270 - User Account Control must run all administrators in Admin Approval Mode, enabling UAC.

Oval ID	Title
oval:mil.disa.stig.windows2019:def:205636	WN19-CC-000370 - Windows Server 2019 Remote Desktop Services must require secure Remote Procedure Call (RPC) communications.
oval:mil.disa.stig.windows2019:def:205876	WN19-DC-000330 - Windows Server 2019 domain controllers must be configured to allow reset of machine account passwords.
oval:mil.disa.stig.windows10:def:220854	WN10-CC-000300 - Basic authentication for RSS feeds over HTTP must not be used.
oval:mil.disa.stig.windows10:def:220945	WN10-SO-000250 - User Account Control must, at minimum, prompt administrators for consent on the secure desktop.
oval:mil.disa.stig.windows2019:def:205680	WN19-00-000350 - Windows Server 2019 must not have Simple TCP/IP Services installed.
oval:mil.disa.stig.windows2019:def:205872	WN19-CC-000330 - Windows Server 2019 File Explorer shell protocol must run in protected mode.
oval:mil.disa.stig.windows2019:def:205747	WN19-MS-000060 - Windows Server 2019 must restrict remote calls to the Security Account Manager (SAM) to Administrators on domain-joined member servers and standalone or nondomain-joined systems.
oval:mil.disa.stig.windows2019:def:205801	WN19-CC-000420 - Windows Server 2019 must prevent users from changing installation options.
oval:mil.disa.stig.windows2019:def:205715	WN19-MS-000020 - Windows Server 2019 local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain-joined member servers.
oval:mil.disa.stig.windows2019:def:205835	WN19-AU-000210 - Windows Server 2019 must be configured to audit Logon/Logoff - Special Logon successes.
oval:mil.disa.stig.windows2019:def:205858	WN19-CC-000030 - Windows Server 2019 Internet Protocol version 6 (IPv6) source routing must be configured to the highest protection level to prevent IP source routing.
oval:mil.disa.stig.windows2019:def:205795	WN19-AC-000010 - Windows Server 2019 account lockout duration must be configured to 15 minutes or greater.
oval:mil.disa.stig.windows2019:def:205719	WN19-SO-000430 - Windows Server 2019 User Account Control (UAC) must only elevate UIAccess applications that are installed in secure locations.
oval:mil.disa.stig.windows10:def:220718	WN10-00-000100 - Internet Information System (IIS) or its subcomponents must not be installed on a workstation.
oval:mil.disa.stig.windows2019:def:205915	WN19-SO-000240 - Windows Server 2019 must be configured to prevent anonymous users from having the same permissions as the Everyone group.
oval:mil.disa.stig.windows2019:def:205659	WN19-AC-000050 - Windows Server 2019 maximum password age must be configured to 60 days or less.
oval:mil.disa.stig.windows10:def:220924	WN10-SO-000095 - The Smart Card removal option must be configured to Force Logoff or Lock Workstation.
oval:mil.disa.stig.windows10:def:220702	WN10-00-000030 - Windows 10 information systems must use BitLocker to encrypt all disks to protect the confidentiality and integrity of all information at rest.
oval:mil.disa.stig.windows2019:def:205823	WN19-SO-000080 - Windows Server 2019 setting Domain member: Digitally sign secure channel data (when possible) must be configured to Enabled.
oval:mil.disa.stig.windows10:def:220926	WN10-SO-000110 - Unencrypted passwords must not be sent to third-party SMB Servers.
oval:mil.disa.stig.windows10:def:220871	WN10-CC-000385 - Windows Ink Workspace must be configured to disallow access above the lock.

Oval ID	Title
oval:mil.disa.stig.windows2019:def:205808	WN19-CC-000340 - Windows Server 2019 must not save passwords in the Remote Desktop Client.
oval:mil.disa.stig.windows10:def:220823	WN10-CC-000155 - Solicited Remote Assistance must not be allowed.
oval:mil.disa.stig.windows10:def:220938	WN10-SO-000205 - The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.
oval:mil.disa.stig.windows2019:def:205791	WN19-DC-000240 - Windows Server 2019 must be configured to audit DS Access - Directory Service Access successes.
oval:mil.disa.stig.windows2019:def:205651	WN19-SO-000350 - Windows Server 2019 users must be required to enter a password to access private keys stored on the computer.
oval:mil.disa.stig.windows10:def:220816	WN10-CC-000105 - Web publishing and online ordering wizards must be prevented from downloading a list of providers.
oval:mil.disa.stig.windows10:def:220783	WN10-AU-000520 - Windows 10 permissions for the Security event log must prevent access by non-privileged accounts.
oval:mil.disa.stig.windows10:def:220831	WN10-CC-000197 - Microsoft consumer experiences must be turned off.
oval:mil.disa.stig.windows10:def:220748	WN10-AU-000005 - The system must be configured to audit Account Logon - Credential Validation failures.
oval:mil.disa.stig.windows2019:def:205769	WN19-AU-000090 - Windows Server 2019 must be configured to audit Account Management - Other Account Management Events successes.
oval:mil.disa.stig.windows10:def:220849	WN10-CC-000275 - Local drives must be prevented from sharing with Remote Desktop Session Hosts.
oval:mil.disa.stig.windows2019:def:205697	WN19-00-000330 - Windows Server 2019 must not have the Microsoft FTP service installed unless required by the organization.
oval:mil.disa.stig.windows10:def:220764	WN10-AU-000084 - Windows 10 must be configured to audit Object Access - Other Object Access Events failures.
oval:mil.disa.stig.windows2019:def:205703	WN19-DC-000030 - Windows Server 2019 Kerberos service ticket maximum lifetime must be limited to 600 minutes or less.
oval:mil.disa.stig.windows2019:def:205776	WN19-AU-000310 - Windows Server 2019 must be configured to audit Privilege Use - Sensitive Privilege Use failures.
oval:mil.disa.stig.windows2019:def:205663	WN19-00-000130 - Windows Server 2019 local volumes must use a format that supports NTFS attributes.
oval:mil.disa.stig.windows10:def:220787	WN10-AU-000560 - Windows 10 must be configured to audit other Logon/Logoff Events Successes.
oval:mil.disa.stig.windows2019:def:205868	WN19-CC-000190 - Windows Server 2019 users must be prompted to authenticate when the system wakes from sleep (plugged in).
oval:mil.disa.stig.windows2019:def:205863	WN19-CC-000100 - Windows Server 2019 must be configured to enable Remote host allows delegation of non-exportable credentials.
oval:mil.disa.stig.windows10:def:220758	WN10-AU-000070 - The system must be configured to audit Logon/Logoff - Logon failures.
oval:mil.disa.stig.windows10:def:220866	WN10-CC-000350 - The Windows Remote Management (WinRM) service must not allow unencrypted traffic.
oval:mil.disa.stig.windows2019:def:205627	WN19-AU-000120 - Windows Server 2019 must be configured to audit Account Management - User Account Management failures.
oval:mil.disa.stig.windows10:def:220730	WN10-00-000165 - The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.

Oval ID	Title
oval:mil.disa.stig.windows2019:def:205862	WN19-CC-000080 - Windows Server 2019 hardened Universal Naming Convention (UNC) paths must be defined to require mutual authentication and integrity for at least the *\SYSVOL and *\NETLOGON shares.
oval:mil.disa.stig.windows2019:def:205779	WN19-AU-000340 - Windows Server 2019 must be configured to audit System - Other System Events successes.
oval:mil.disa.stig.windows10:def:220934	WN10-SO-000180 - NTLM must be prevented from falling back to a Null session.
oval:mil.disa.stig.windows2019:def:205705	WN19-DC-000050 - Windows Server 2019 Kerberos policy user ticket renewal maximum lifetime must be limited to seven days or less.
oval:mil.disa.stig.windows10:def:220808	WN10-CC-000065 - Wi-Fi Sense must be disabled.
oval:mil.disa.stig.windows2019:def:205628	WN19-DC-000230 - Windows Server 2019 must be configured to audit Account Management - Computer Account Management successes.
oval:mil.disa.stig.windows2019:def:205906	WN19-MS-000050 - Windows Server 2019 must limit the caching of logon credentials to four or less on domain-joined member servers.
oval:mil.disa.stig.windows10:def:220827	WN10-CC-000180 - Autoplay must be turned off for non-volume devices.
oval:mil.disa.stig.windows10:def:220844	WN10-CC-000250 - The Windows Defender SmartScreen filter for Microsoft Edge must be enabled.
oval:mil.disa.stig.defs:def:220844	The Windows Defender SmartScreen filter for Microsoft Edge must be enabled.
oval:mil.disa.stig.windows2019:def:205775	WN19-AU-000300 - Windows Server 2019 must be configured to audit Privilege Use - Sensitive Privilege Use successes.
oval:mil.disa.stig.windows2019:def:205826	WN19-SO-000170 - Windows Server 2019 setting Microsoft network client: Digitally sign communications (if server agrees) must be configured to Enabled.
oval:mil.disa.stig.windows2019:def:205653	WN19-AC-000090 - Windows Server 2019 reversible password encryption must be disabled.
oval:mil.disa.stig.windows10:def:220856	WN10-CC-000310 - Users must be prevented from changing installation options.
oval:mil.disa.stig.windows10:def:220927	WN10-SO-000120 - The Windows SMB server must be configured to always perform SMB packet signing.
oval:mil.disa.stig.windows10:def:220810	WN10-CC-000068 - Windows 10 must be configured to enable Remote host allows delegation of non-exportable credentials.
oval:mil.disa.stig.windows10:def:220870	WN10-CC-000370 - The convenience PIN for Windows 10 must be disabled.
oval:mil.disa.stig.windows10:def:220704	WN10-00-000032 - Windows 10 systems must use a BitLocker PIN with a minimum length of six digits for pre-boot authentication.
oval:mil.disa.stig.windows10:def:220925	WN10-SO-000100 - The Windows SMB client must be configured to always perform SMB packet signing.
oval:mil.disa.stig.windows2019:def:205724	WN19-SO-000230 - Windows Server 2019 must not allow anonymous enumeration of shares.
oval:mil.disa.stig.windows2019:def:205722	WN19-CC-000350 - Windows Server 2019 Remote Desktop Services must prevent drive redirection.
oval:mil.disa.stig.windows2019:def:205819	WN19-CC-000060 - Windows Server 2019 must be configured to ignore NetBIOS name release requests except from WINS servers.
oval:mil.disa.stig.windows10:def:220825	WN10-CC-000170 - The setting to allow Microsoft accounts to be optional for modern style apps must be enabled.
oval:mil.disa.stig.windows10:def:220923	WN10-SO-000085 - Caching of logon credentials must be limited.

Oval ID	Title
oval:mil.disa.stig.windows2019:def:205683	WN19-00-000390 - Windows Server 2019 must have the Server Message Block (SMB) v1 protocol disabled on the SMB server.
oval:mil.disa.stig.windows10:def:220845	WN10-CC-000252 - Windows 10 must be configured to disable Windows Game Recording and Broadcasting.
oval:mil.disa.stig.windows10:def:220853	WN10-CC-000295 - Attachments must be prevented from being downloaded from RSS feeds.
oval:mil.disa.stig.windows10:def:220837	WN10-CC-000215 - Explorer Data Execution Prevention must be enabled.
oval:mil.disa.stig.windows2019:def:205849	WN19-00-000100 - Windows Server 2019 must be maintained at a supported servicing level.
oval:mil.disa.stig.defs:def:205849	Windows must be maintained at a supported servicing level.
oval:mil.disa.stig.windows10:def:220943	WN10-SO-000240 - The default permissions of global system objects must be increased.
oval:mil.disa.stig.windows2019:def:205908	WN19-SO-000020 - Windows Server 2019 must prevent local accounts with blank passwords from being used from the network.
oval:mil.disa.stig.windows2019:def:205817	WN19-CC-000510 - Windows Server 2019 Windows Remote Management (WinRM) service must not allow unencrypted traffic.
oval:mil.disa.stig.windows10:def:220817	WN10-CC-000110 - Printing over HTTP must be prevented.
oval:mil.disa.stig.windows10:def:220749	WN10-AU-000010 - The system must be configured to audit Account Logon - Credential Validation successes.
oval:mil.disa.stig.windows10:def:220838	WN10-CC-000220 - Turning off File Explorer heap termination on corruption must be disabled.
oval:mil.disa.stig.windows10:def:220719	WN10-00-000105 - Simple Network Management Protocol (SNMP) must not be installed on the system.
oval:mil.disa.stig.defs:def:220719	Simple Network Management Protocol (SNMP) must not be installed on the system.
oval:mil.disa.stig.windows2019:def:205625	WN19-AU-000100 - Windows Server 2019 must be configured to audit Account Management - Security Group Management successes.
oval:mil.disa.stig.windows10:def:220759	WN10-AU-000075 - The system must be configured to audit Logon/Logoff - Logon successes.
oval:mil.disa.stig.windows10:def:220820	WN10-CC-000130 - Local users on domain-joined computers must not be enumerated.
oval:mil.disa.stig.windows10:def:220814	WN10-CC-000090 - Group Policy objects must be reprocessed even if they have not changed.
oval:mil.disa.stig.windows10:def:220750	WN10-AU-000030 - The system must be configured to audit Account Management - Security Group Management successes.
oval:mil.disa.stig.windows10:def:220951	WN10-SO-000275 - User Account Control must virtualize file and registry write failures to per-user locations.
oval:mil.disa.stig.windows2019:def:205812	WN19-SO-000410 - Windows Server 2019 User Account Control must automatically deny standard user requests for elevation.
oval:mil.disa.stig.windows10:def:220781	WN10-AU-000510 - The System event log size must be configured to 32768 KB or greater.
oval:mil.disa.stig.windows2019:def:205805	WN19-CC-000220 - Windows Server 2019 default AutoRun behavior must be configured to prevent AutoRun commands.

Oval ID	Title
oval:mil.disa.stig.windows10:def:220780	WN10-AU-000505 - The Security event log size must be configured to 1024000 KB or greater.
oval:mil.disa.stig.windows2019:def:205684	WN19-00-000400 - Windows Server 2019 must have the Server Message Block (SMB) v1 protocol disabled on the SMB client.
oval:mil.disa.stig.windows10:def:220855	WN10-CC-000305 - Indexing of encrypted files must be turned off.
oval:mil.disa.stig.windows10:def:220769	WN10-AU-000107 - The system must be configured to audit Policy Change - Authorization Policy Change successes.
oval:mil.disa.stig.windows2019:def:205679	WN19-00-000340 - Windows Server 2019 must not have the Peer Name Resolution Protocol installed.
oval:mil.disa.stig.windows10:def:220859	WN10-CC-000325 - Automatically signing in the last interactive user after a system-initiated restart must be disabled.
oval:mil.disa.stig.windows2019:def:205709	WN19-SO-000010 - Windows Server 2019 must have the built-in guest account disabled.
oval:mil.disa.stig.windows2019:def:205874	WN19-CC-000440 - Windows Server 2019 users must be notified if a web-based program attempts to install software.
oval:mil.disa.stig.windows10:def:220784	WN10-AU-000525 - Windows 10 permissions for the System event log must prevent access by non-privileged accounts.
oval:mil.disa.stig.windows2019:def:205774	WN19-AU-000290 - Windows Server 2019 must be configured to audit Policy Change - Authorization Policy Change successes.
oval:mil.disa.stig.windows2019:def:205698	WN19-00-000360 - Windows Server 2019 must not have the Telnet Client installed.
oval:mil.disa.stig.windows2019:def:205802	WN19-CC-000430 - Windows Server 2019 must disable the Windows Installer Always install with elevated privileges option.
oval:mil.disa.stig.windows10:def:220839	WN10-CC-000225 - File Explorer shell protocol must run in protected mode.
oval:mil.disa.stig.windows10:def:220939	WN10-SO-000210 - The system must be configured to the required LDAP client signing level.
oval:mil.disa.stig.windows10:def:250319	WN10-CC-000050 - Hardened UNC paths must be defined to require mutual authentication and integrity for at least the *\SYSVOL and *\NETLOGON shares.
oval:mil.disa.stig.windows2019:def:205813	WN19-SO-000440 - Windows Server 2019 User Account Control must run all administrators in Admin Approval Mode, enabling UAC.
oval:mil.disa.stig.windows10:def:220803	WN10-CC-000044 - Internet connection sharing must be disabled.
oval:mil.disa.stig.windows2019:def:205696	WN19-MS-000030 - Windows Server 2019 local users on domain-joined member servers must not be enumerated.
oval:mil.disa.stig.windows10:def:220726	WN10-00-000145 - Data Execution Prevention (DEP) must be configured to at least OptOut.
oval:mil.disa.stig.windows2019:def:205912	WN19-SO-000150 - Windows Server 2019 Smart Card removal option must be configured to Force Logoff or Lock Workstation.
oval:mil.disa.stig.windows10:def:220800	WN10-CC-000038 - WDigest Authentication must be disabled.
oval:mil.disa.stig.windows2019:def:205921	WN19-SO-000330 - Windows Server 2019 session security for NTLM SSP-based clients must be configured to require NTLMv2 session security and 128-bit encryption.
oval:mil.disa.stig.windows10:def:220824	WN10-CC-000165 - Unauthenticated RPC clients must be restricted from connecting to the RPC server.

Oval ID	Title
oval:mil.disa.stig.windows2019:def:205809	WN19-CC-000360 - Windows Server 2019 Remote Desktop Services must always prompt a client for passwords upon connection.
oval:mil.disa.stig.windows2019:def:205911	WN19-SO-000100 - Windows Server 2019 maximum age for machine account passwords must be configured to 30 days or less.
oval:mil.disa.stig.windows2019:def:205714	WN19-CC-000240 - Windows Server 2019 administrator accounts must not be enumerated during elevation.
oval:mil.disa.stig.windows10:def:220930	WN10-SO-000150 - Anonymous enumeration of shares must be restricted.
oval:mil.disa.stig.windows10:def:220782	WN10-AU-000515 - Windows 10 permissions for the Application event log must prevent access by non-privileged accounts.
oval:mil.disa.stig.windows2019:def:205691	WN19-CC-000200 - Windows Server 2019 Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.
oval:mil.disa.stig.windows10:def:220868	WN10-CC-000360 - The Windows Remote Management (WinRM) client must not use Digest authentication.
oval:mil.disa.stig.windows2019:def:205682	WN19-00-000380 - Windows Server 2019 must not have the Server Message Block (SMB) v1 protocol installed.
oval:mil.disa.stig.windows2019:def:205804	WN19-CC-000210 - Windows Server 2019 Autoplay must be turned off for non-volume devices.
oval:mil.disa.stig.windows10:def:220791	WN10-AU-000580 - Windows 10 must be configured to audit MPSSVC Rule-Level Policy Change Failures.
oval:mil.disa.stig.windows10:def:220743	WN10-AC-000025 - The maximum password age must be configured to 60 days or less.
oval:mil.disa.stig.windows10:def:220731	WN10-00-000170 - The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.
oval:mil.disa.stig.windows10:def:220929	WN10-SO-000145 - Anonymous enumeration of SAM accounts must not be allowed.
oval:mil.disa.stig.windows10:def:220739	WN10-AC-000005 - Windows 10 account lockout duration must be configured to 15 minutes or greater.
oval:mil.disa.stig.windows10:def:220858	WN10-CC-000320 - Users must be notified if a web-based program attempts to install software.
oval:mil.disa.stig.windows10:def:220821	WN10-CC-000145 - Users must be prompted for a password on resume from sleep (on battery).
oval:mil.disa.stig.windows10:def:220902	WN10-EP-000310 - Windows 10 Kernel (Direct Memory Access) DMA Protection must be enabled.
oval:mil.disa.stig.windows10:def:220763	WN10-AU-000083 - Windows 10 must be configured to audit Object Access - Other Object Access Events successes.
oval:mil.disa.stig.windows2019:def:205730	WN19-AU-000160 - Windows Server 2019 must be configured to audit Logon/Logoff - Account Lockout failures.
oval:mil.disa.stig.windows10:def:220732	WN10-00-000175 - The Secondary Logon service must be disabled on Windows 10.
oval:mil.disa.stig.windows2019:def:205782	WN19-AU-000370 - Windows Server 2019 must be configured to audit System - Security System Extension successes.
oval:mil.disa.stig.windows10:def:220767	WN10-AU-000100 - The system must be configured to audit Policy Change - Audit Policy Change successes.

Oval ID	Title
oval:mil.disa.stig.windows10:def:220797	WN10-CC-000030 - The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.
oval:mil.disa.stig.windows10:def:220721	WN10-00-000115 - The Telnet Client must not be installed on the system.
oval:mil.disa.stig.windows2019:def:205685	WN19-00-000410 - Windows Server 2019 must not have Windows PowerShell 2.0 installed.
oval:mil.disa.stig.defs:def:205685	The Windows PowerShell 2.0 feature must be disabled on the system.
oval:mil.disa.stig.windows10:def:220772	WN10-AU-000120 - The system must be configured to audit System - IPSec Driver failures.
oval:mil.disa.stig.windows2019:def:205919	WN19-SO-000310 - Windows Server 2019 LAN Manager authentication level must be configured to send NTLMv2 response only and to refuse LM and NTLM.
oval:mil.disa.stig.windows10:def:220741	WN10-AC-000015 - The period of time before the bad logon counter is reset must be configured to 15 minutes.
oval:mil.disa.stig.windows2019:def:205918	WN19-SO-000280 - Windows Server 2019 must prevent PKU2U authentication using online identities.
oval:mil.disa.stig.windows10:def:220848	WN10-CC-000270 - Passwords must not be saved in the Remote Desktop Client.
oval:mil.disa.stig.windows10:def:220933	WN10-SO-000167 - Remote calls to the Security Account Manager (SAM) must be restricted to Administrators.
oval:mil.disa.stig.windows2019:def:205837	WN19-AU-000230 - Windows Server 2019 must be configured to audit Object Access - Other Object Access Events failures.
oval:mil.disa.stig.windows2019:def:205909	WN19-SO-000030 - Windows Server 2019 built-in administrator account must be renamed.

Updated Benchmarks

Benchmark ID	Title
AppleMacOSXPatchPolicy	Apple Mac OSX Patch Policy
LatestPatchPolicyBenchmark	Latest Patch Policy Benchmark - 09.03.2025

DISA STIG Benchmarks

Red Hat Enterprise Linux 7 STIG Benchmark - Ver 3, Rel 15	5th November 2024
Red Hat Enterprise Linux 8 STIG Benchmark - Ver 2, Rel 4	3rd September 2025
Red Hat Enterprise Linux 9 STIG Benchmark - Ver 2, Rel 5	3rd September 2025
Canonical Ubuntu 20.04 LTS STIG SCAP Benchmark – Ver 2, Rel 4	3rd September 2025
Canonical Ubuntu 18.04 LTS STIG SCAP Benchmark – Ver 2, Rel 11	2nd February 2024
Microsoft Windows 10 STIG Benchmark - Ver 3, Rel 5	3rd September 2025
Microsoft Windows 2012 and 2012 R2 MS STIG Benchmark - Ver 3, Rel 5	12th May 2023
Microsoft Windows 2012 and 2012 R2 DC STIG Benchmark - Ver 3, Rel 5	12th May 2023

Microsoft Windows Server 2019 STIG Benchmark – Ver 3, Rel 5	3rd September 2025
Microsoft Windows Server 2016 STIG Benchmark - Ver 2, Rel 7	5th November 2024
Microsoft Windows 11 STIG Benchmark - Ver 2, Rel 5	3rd September 2025
Microsoft Windows Server 2022 STIG Benchmark – Ver 2, Rel 5	3rd September 2025
Windows 8 and 8-1 STIG Benchmark - Ver 1, Rel 22	11th June 2021
Red Hat Enterprise Linux 6 STIG Benchmark - Ver 2, Rel 2	26th February 2021
Microsoft Windows 2008 R2 DC STIG Benchmark - Ver 1, Rel 32	9th August 2019
Microsoft Windows 2008 R2 MS STIG Benchmark - Ver 1, Rel 33	9th August 2019
Canonical Ubuntu 22.04 LTS STIG SCAP Benchmark – Ver 2, Rel 3	19th May 2025

Trellix Technical Support

PrimeSupport ServicePortal: https://supportm.trellix.com

This message may contain confidential and privileged material for the sole use of the intended recipient. Any review or distribution by others is strictly prohibited. If you are not the intended recipient please contact the sender and delete all copies.