Non-Compliance Report - Windows_10_STIG

SCAP Compliance Checker - 5.3.1

Score

97.16%

Adjusted Score: 97.16%
Original Score: 97.16%
Compliance Status: GREEN

Pass:	205	Not Applicable:	0
Fail:	6	Not Checked:	0
Error:	0	Not Selected:	0
Unknown:	0	Informational:	0
Fixed:	0	Total:	211

BLUE:	Score equals 100
GREEN:	Score is greater than or equal to 90
YELLOW:	Score is greater than or equal to 80
RED:	Score is greater than or equal to 0

System Information

Target Hostname:	D21-S1-demo
Operating System:	Windows 10 Enterprise
OS Version:	1909
Domain:	demo.demo
FQDN:	D21-S1-demo.demo.demo

Processor:	Intel(R) Core(TM) i7-7700 CPU @ 3.60GHz
Processor Architecture:	Intel64 Family 6 Model 158 Stepping 9
Processor Speed:	3600 mhz
Physical Memory:	16384 mb
Manufacturer:	DFI Inc.
Model:	
Serial Number:	123456789
BIOS Version:	B192.19A

Interfaces:	• [00000001] Intel(R) Ethernet Connection (2) I219-LM
	  ◦ IP Addresses
	  ▪ 192.168.16.1
	  ◦ MAC Address: Redacted
	• [00000008] WAN Miniport (IP)
	  ◦ IP Addresses
	  ▪ IP not found.
	  ◦ MAC Address: redacted
	• [00000009] WAN Miniport (IPv6)
	  ◦ IP Addresses
	  ▪ IP not found.
	  ◦ MAC Address: redacted
	• [00000010] WAN Miniport (Network Monitor)
	  ◦ IP Addresses
	  ▪ IP not found.
	  ◦ MAC Address: redacted
	• [00000011] RAS Async Adapter
	  ◦ IP Addresses
	  ▪ IP not found.
	  ◦ MAC Address: redacted

Content Information

Stream:	Windows_10_STIG
Profile:	Id: MAC-1_Classified
Digital Signature Status:	NOT DIGITALLY SIGNED

Stream Installation Date:	2021-03-09
Status:	accepted (2020-10-15)
Title:	Windows 10 Security Technical Implementation Guide
Description:	This Security Technical Implementation Guide is published as a tool to improve the security of Department of Defense (DoD) information systems. The requirements are derived from the National Institute of Standards and Technology (NIST) 800-53 and related documents. Comments or proposed revisions to this document should be sent via email to the following address: disa.stig_spt@mail.mil.
Notice:	
Target Platforms:	• cpe:/o:microsoft:windows_10
Reference:	Href: https://cyber.mil Publisher: DISA Source: STIG.DOD.MIL
Stream Version:	002.001
Start Time:	2021-03-09T11:33:23
End Time:	2021-03-09T11:33:40
Scanner:	cpe:/a:spawar:scc:5.3.1
Identity:	demo\helpdesk
Identity Privileged:	true
Identity Authenticated:	true
Release Info:	Release: 2.1 Benchmark Date: 13 Nov 2020

Results

- **SRG-OS-000185-GPOS-00079**
  - Windows 10 information systems must use BitLocker to encrypt all disks to protect the confidentiality and integrity of all information at rest. - Fail
- **SRG-OS-000076-GPOS-00044**
  - Accounts must be configured to require password expiration. - Fail
- **SRG-OS-000029-GPOS-00010**
  - The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver. - (CCE-47830-5) - Fail
- **SRG-OS-000080-GPOS-00048**
  - 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. - Fail
- **SRG-OS-000080-GPOS-00048**

- 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. - Fail

- **SRG-OS-000080-GPOS-00048**
  - 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. - Fail

Detailed Results

Windows 10 information systems must use BitLocker to encrypt all disks to protect the confidentiality and integrity of all information at rest.

Rule ID:	xccdf_mil.disa.stig_rule_SV-220702r569228_rule
Result:	Fail
Version:	WN10-00-000030
Identities:	SV-77827 V-63337 CCI-001199 (NIST SP 800-53: SC-28; NIST SP 800-53A: SC-28.1; NIST SP 800-53 Rev 4: SC-28) CCI-002475 (NIST SP 800-53 Rev 4: SC-28 (1)) CCI-002476 (NIST SP 800-53 Rev 4: SC-28 (1))
Description:	If data at rest is unencrypted, it is vulnerable to disclosure. Even if the operating system enforces permissions on data access, an adversary can remove non-volatile memory and read it directly, thereby circumventing operating system controls. Encrypting the data ensures that confidentiality is protected even when the operating system is not running. false
Fix Text:	Enable full disk encryption on all information systems (including SIPRNet) using BitLocker. BitLocker, included in Windows, can be enabled in the Control Panel under "BitLocker Drive Encryption" as well as other management tools. NOTE: An alternate encryption application may be used in lieu of BitLocker providing it is configured for full disk encryption and satisfies the pre-boot authentication requirements (WN10-00-000031 and WN10-00-000032).
Severity:	medium
Weight:	10.0
Reference:	Title: DPMS Target Windows 10 Publisher: DISA Type: DPMS Target Subject: Windows 10 Identifier: 4072

Definitions:	Definition ID: oval:mil.disa.stig.windows:def:177 Result: false Title: BitLocker must be enabled on all fixed drives. Description: BitLocker must be enabled on all fixed drives. Class: compliance Tests: • false (All child checks must be true.) ◦ false (BitLocker must be enabled on all fixed drives.)
Tests:	Test ID: oval:mil.disa.stig.windows:tst:17700 (wmi57_test) Result: false Title: BitLocker must be enabled on all fixed drives. Check Existence: All collected items must exist. Check: All collected items must match the given state(s). Object ID: oval:mil.disa.stig.windows:obj:17700 (wmi57_object) Object Requirements: • namespace must be equal to 'root\cimv2\security\microsoftvolumeencryption' • wql must be equal to 'SELECT protectionstatus FROM win32_encryptablevolume' State ID: oval:mil.disa.stig.windows:ste:17700 (wmi57_state) State Requirements: • for all 'result' the following must be true: ◦ protectionstatus must be equal to '1' Collected Item Properties: • namespace equals 'root\cimv2\security\microsoftvolumeencryption' • wql equals 'SELECT protectionstatus FROM win32_encryptablevolume' • collected 'result' result: ◦ protectionstatus = '0' • collected 'result' result: ◦ protectionstatus = '0' Additional Information: Check requirement not met.

Accounts must be configured to require password expiration.

Rule ID:	xccdf_mil.disa.stig_rule_SV-220716r569187_rule
Result:	Fail
Version:	WN10-00-000090
Identities:	V-63371 SV-77861 CCI-000199 (NIST SP 800-53: IA-5 (1) (d); NIST SP 800-53A: IA-5 (1).1 (v); NIST SP 800-53 Rev 4: IA-5 (1) (d))
Description:	Passwords that do not expire increase exposure with a greater probability of being discovered or cracked. false
Fix Text:	Configure all passwords to expire. Run "Computer Management". Navigate to System Tools >> Local Users and Groups >> Users. Double click each active account. Ensure "Password never expires" is not checked on all active accounts.

Severity:	medium
Weight:	10.0
Reference:	Title: DPMS Target Windows 10 Publisher: DISA Type: DPMS Target Subject: Windows 10 Identifier: 4072
Definitions:	Definition ID: oval:mil.disa.stig.windows:def:77 Result: false Title: Accounts must be configured to require password expiration. Description: Accounts must be configured to require password expiration. Class: compliance Tests: • false (All child checks must be true.) ◦ false (No active, local accounts have non-expiring passwords.)
Tests:	Test ID: oval:mil.disa.stig.windows:tst:7700 (wmi_test) Result: false Title: No active, local accounts have non-expiring passwords. Check Existence: No collected items may exist. Check: Result is based on check existence only. Object ID: oval:mil.disa.stig.windows:obj:7700 (wmi_object) Object Requirements: • namespace must be equal to 'root\cimv2' • wql must be equal to 'SELECT name FROM Win32_UserAccount WHERE LocalAccount=TRUE AND Disabled=FALSE AND PasswordExpires=FALSE' Collected Item Properties: • namespace equals 'root\cimv2' • wql equals 'SELECT name FROM Win32_UserAccount WHERE LocalAccount=TRUE AND Disabled=FALSE AND PasswordExpires=FALSE' • result equals 'administrator' • result equals 'd21user' • result equals 'helpdesk' • result equals 'masterlock' • result equals 'demoadmin' • result equals 'demoServiceApp' • result equals 'Monaco' Additional Information: Check existence requirement not met.

The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.

Rule ID:	xccdf_mil.disa.stig_rule_SV-220920r569187_rule
Result:	Fail
Version:	WN10-SO-000070

Identities:	CCE-47830-5 V-63669 SV-78159 CCI-000057 (NIST SP 800-53: AC-11 a; NIST SP 800-53A: AC-11.1 (ii); NIST SP 800-53 Rev 4: AC-11 a)
Description:	Unattended systems are susceptible to unauthorized use and should be locked when unattended. The screen saver should be set at a maximum of 15 minutes and be password protected. This protects critical and sensitive data from exposure to unauthorized personnel with physical access to the computer. false
Fix Text:	Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> "Interactive logon: Machine inactivity limit" to "900" seconds" or less, excluding "0" which is effectively disabled.
Severity:	medium
Weight:	10.0
Reference:	Title: DPMS Target Windows 10 Publisher: DISA Type: DPMS Target Subject: Windows 10 Identifier: 4072
Definitions:	Definition ID: oval:mil.disa.fso.windows:def:4730 Result: false Title: WN10-SO-000070 Description: The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver. Class: compliance Tests: • false (All child checks must be true.) ◦ false (All child checks must be true.) ▪ false ('Interactive logon: Machine inactivity limit' is set to '900' seconds or less)
Tests:	Test ID: oval:mil.disa.stig.windows:tst:420200 (registry_test) Result: false Title: 'Interactive logon: Machine inactivity limit' is set to '900' seconds or less Check Existence: One or more collected items must exist. Check: All collected items must match the given state(s). State Operator: All item-state comparisons must be true. Object ID: oval:mil.disa.stig.windows:obj:420200 (registry_object) Object Requirements: • hive must be equal to 'HKEY_LOCAL_MACHINE' • key must be equal to 'Software\Microsoft\Windows\CurrentVersion\Policies\System' • name must be equal to 'InactivityTimeoutSecs' State ID: oval:mil.disa.stig.windows:ste:420200 (registry_state) State Requirements: • all type must be equal to 'reg_dword' • all value must be less than or equal to '900' State ID: oval:mil.disa.stig.windows:ste:420201 (registry_state) State Requirements: • all type must be equal to 'reg_dword' • all value must be greater than '0' Collected Item Properties: • hive equals 'HKEY_LOCAL_MACHINE' • key equals 'Software\Microsoft\Windows\CurrentVersion\Policies\System' • name equals 'InactivityTimeoutSecs' • last_write_time equals '132597178270000000'

	• type equals 'reg_dword' • value equals '0' • windows_view equals '64_bit' Additional Information: Check requirement not met.

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.

Rule ID:	xccdf_mil.disa.stig_rule_SV-220968r569187_rule
Result:	Fail
Version:	WN10-UR-000070
Identities:	SV-78361 V-63871 CCI-000213 (NIST SP 800-53: AC-3; NIST SP 800-53A: AC-3.1; NIST SP 800-53 Rev 4: AC-3)
Description:	Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities. The "Deny access to this computer from the network" right defines the accounts that are prevented from logging on from the network. In an Active Directory Domain, denying logons to the Enterprise Admins and Domain Admins groups on lower trust systems helps mitigate the risk of privilege escalation from credential theft attacks, which could lead to the compromise of an entire domain. Local accounts on domain-joined systems must also be assigned this right to decrease the risk of lateral movement resulting from credential theft attacks. The Guests group must be assigned this right to prevent unauthenticated access. false
Fix Text:	Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> "Deny access to this computer from the network" to include the following. Domain Systems Only: Enterprise Admins group Domain Admins group Local account (see Note below) All Systems: Guests group Privileged Access Workstations (PAWs) dedicated to the management of Active Directory are exempt from denying the Enterprise Admins and Domain Admins groups. (See the Windows Privileged Access Workstation STIG for PAW requirements.) Note: "Local account" is a built-in security group used to assign user rights and permissions to all local accounts.
Severity:	medium

Weight:	10.0
Reference:	Title: DPMS Target Windows 10 Publisher: DISA Type: DPMS Target Subject: Windows 10 Identifier: 4072
Definitions:	Definition ID: oval:mil.disa.fso.windows:def:4775 Result: false Title: UR: Deny access to this computer from the network Description: 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 administrator accounts on domain systems and unauthenticated access on all systems. Class: compliance Tests: • false (One or more child checks must be true.) ◦ false (All child checks must be true.) ▪ true (Deny access to this computer from the network - Guests) ▪ false (All child checks must be true.) ▪ false (System is not a member of a domain) ◦ false (All child checks must be true.) ▪ true (Deny access to this computer from the network - Guests) ▪ false (Deny access to this computer from the network - Domain Admins) ▪ false (Deny access to this computer from the network - Enterprise Admins) ▪ false (Deny access to this computer from the network - Local account) ▪ true (All child checks must be true.) (negated) ▪ false (System is not a member of a domain)
Tests:	Test ID: oval:mil.disa.fso.windows:tst:477500 (accesstoken_test) Result: true Title: Deny access to this computer from the network - Guests Check Existence: One or more collected items must exist. Check: All collected items must match the given state(s). Object ID: oval:mil.disa.fso.windows:obj:437001 (accesstoken_object) Object Requirements: • security_principle must be equal to 'Guests' State ID: oval:mil.disa.fso.windows:ste:477500 (accesstoken_state) State Requirements: • all sedenynetworklogonright must be equal to '1' Test ID: oval:mil.disa.fso.windows:tst:498200 (wmi_test) Result: false Title: System is not a member of a domain Check Existence: One or more collected items must exist. Check: All collected items must match the given state(s). State Operator: One or more item-state comparisons may be true. Object ID: oval:mil.disa.fso.windows:obj:498200 (wmi_object) Object Requirements: • namespace must be equal to 'root\cimv2' • wql must be equal to 'SELECT DomainRole FROM win32_computersystem' State ID: oval:mil.disa.fso.windows:ste:498200 (wmi_state) State Requirements: • all result must be equal to '0' State ID: oval:mil.disa.fso.windows:ste:498203 (wmi_state)

State Requirements:
- all result must be equal to '2'

Collected Item Properties:
- namespace equals 'root\cimv2'
- wql equals 'SELECT DomainRole FROM win32_computersystem'
- result equals '1'

Additional Information: Check requirement not met.

Test ID: oval:mil.disa.fso.windows:tst:477501 (accesstoken_test)
Result: false
Title: Deny access to this computer from the network - Domain Admins
Check Existence: One or more collected items must exist.
Check: At least one collected item must match the given state(s).
Object ID: oval:mil.disa.fso.windows:obj:477500 (accesstoken_object)

Object Requirements:
- Collect any available items.

State ID: oval:mil.disa.fso.windows:ste:477500 (accesstoken_state)

State Requirements:
- all sedenynetworklogonright must be equal to '1'

Collected Item Properties:
- Message - 'security_principle'
- security_principle equals 'Domain Admins'
- seassignprimarytokenprivilege equals '0'
- seauditprivilege equals '0'
- sebackupprivilege equals '0'
- sechangenotifyprivilege equals '0'
- secreateglobalprivilege equals '0'
- secreatepagefileprivilege equals '0'
- secreatepermanentprivilege equals '0'
- secreatesymboliclinkprivilege equals '0'
- secreatetokenprivilege equals '0'
- sedebugprivilege equals '0'
- seenabledelegationprivilege equals '0'
- seimpersonateprivilege equals '0'
- seincreasebaseprioritytprivilege equals '0'
- seincreasequotaprivilege equals '0'
- seincreaseworkingsetprivilege equals '0'
- seloaddriverprivilege equals '0'
- selockmemoryprivilege equals '0'
- semachineaccountprivilege equals '0'
- semanagevolumeprivilege equals '0'
- seprofilesingleprocessprivilege equals '0'
- serelabelprivilege equals '0'
- seremoteshutdownprivilege equals '0'
- serestoreprivilege equals '0'
- sesecurityprivilege equals '0'
- seshutdownprivilege equals '0'
- sesyncagentprivilege equals '0'
- sesystemenvironmentprivilege equals '0'
- sesystemprofileprivilege equals '0'
- sesystemtimeprivilege equals '0'
- setakeownershipprivilege equals '0'
- setcbprivilege equals '0'

- setimezoneprivilege equals '0'
- seundockprivilege equals '0'
- seunsolicitedinputprivilege equals '0'
- sebatchlogonright equals '0'
- seinteractivelogonright equals '0'
- senetworklogonright equals '0'
- seremoteinteractivelogonright equals '0'
- seservicelogonright equals '0'
- sedenybatchLogonright equals '1'
- sedenyinteractivelogonright equals '0'
- sedenynetworklogonright equals '0'
- sedenyremoteInteractivelogonright equals '0'
- sedenyservicelogonright equals '0'
- setrustedcredmanaccessnameright equals '0'

Additional Information: Check requirement not met.

Test ID: oval:mil.disa.fso.windows:tst:477502 (accesstoken_test)
Result: false
Title: Deny access to this computer from the network - Enterprise Admins
Check Existence: One or more collected items must exist.
Check: At least one collected item must match the given state(s).
Object ID: oval:mil.disa.fso.windows:obj:477501 (accesstoken_object)
Object Requirements:
- Collect any available items.

State ID: oval:mil.disa.fso.windows:ste:477500 (accesstoken_state)
State Requirements:
- all sedenynetworklogonright must be equal to '1'

Collected Item Properties:
- Message - 'security_principle'
- security_principle equals 'Enterprise Admins'
- seassignprimarytokenprivilege equals '0'
- seauditprivilege equals '0'
- sebackupprivilege equals '0'
- sechangenotifyprivilege equals '0'
- secreateglobalprivilege equals '0'
- secreatepagefileprivilege equals '0'
- secreatepermanentprivilege equals '0'
- secreatesymboliclinkprivilege equals '0'
- secreatetokenprivilege equals '0'
- sedebugprivilege equals '0'
- seenabledelegationprivilege equals '0'
- seimpersonateprivilege equals '0'
- seincreasebaseprioritytprivilege equals '0'
- seincreasequotaprivilege equals '0'
- seincreaseworkingsetprivilege equals '0'
- seloaddriverprivilege equals '0'
- selockmemoryprivilege equals '0'
- semachineaccountprivilege equals '0'
- semanagevolumeprivilege equals '0'
- seprofilesingleprocessprivilege equals '0'
- serelabelprivilege equals '0'

- seremoteshutdownprivilege equals '0'
- serestoreprivilege equals '0'
- sesecurityprivilege equals '0'
- seshutdownprivilege equals '0'
- sesyncagentprivilege equals '0'
- sesystemenvironmentprivilege equals '0'
- sesystemprofileprivilege equals '0'
- sesystemtimeprivilege equals '0'
- setakeownershipprivilege equals '0'
- setcbprivilege equals '0'
- setimezoneprivilege equals '0'
- seundockprivilege equals '0'
- seunsolicitedinputprivilege equals '0'
- sebatchlogonright equals '0'
- seinteractivelogonright equals '0'
- senetworklogonright equals '0'
- seremoteinteractivelogonright equals '0'
- seservicelogonright equals '0'
- sedenybatchLogonright equals '1'
- sedenyinteractivelogonright equals '0'
- sedenynetworklogonright equals '0'
- sedenyremoteInteractivelogonright equals '0'
- sedenyservicelogonright equals '0'
- setrustedcredmanaccessnameright equals '0'

Additional Information: Check requirement not met.

Test ID: oval:mil.disa.fso.windows:tst:477508 (accesstoken_test)
Result: false
Title: Deny access to this computer from the network - Local account
Check Existence: One or more collected items must exist.
Check: All collected items must match the given state(s).
Object ID: oval:mil.disa.fso.windows:obj:477509 (accesstoken_object)
Object Requirements:
- Collect any available items.

State ID: oval:mil.disa.fso.windows:ste:477500 (accesstoken_state)
State Requirements:
- all sedenynetworklogonright must be equal to '1'

Additional Information: Check existence requirement not met.

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.

Rule ID:	xccdf_mil.disa.stig_rule_SV-220970r569187_rule
Result:	Fail
Version:	WN10-UR-000080

Identities:	SV-78365 V-63875 CCI-000213 (NIST SP 800-53: AC-3; NIST SP 800-53A: AC-3.1; NIST SP 800-53 Rev 4: AC-3)
Description:	Inappropriate granting of user rights can provide system, administrative, and other high level capabilities. The "Deny log on as a service" right defines accounts that are denied log on as a service. In an Active Directory Domain, denying logons to the Enterprise Admins and Domain Admins groups on lower trust systems helps mitigate the risk of privilege escalation from credential theft attacks which could lead to the compromise of an entire domain. Incorrect configurations could prevent services from starting and result in a DoS. false
Fix Text:	This requirement is applicable to domain-joined systems, for standalone systems this is NA. Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> "Deny log on as a service" to include the following. Domain Systems Only: Enterprise Admins Group Domain Admins Group
Severity:	medium
Weight:	10.0
Reference:	Title: DPMS Target Windows 10 Publisher: DISA Type: DPMS Target Subject: Windows 10 Identifier: 4072
Definitions:	Definition ID: oval:mil.disa.fso.windows:def:4372 Result: false Title: UR: Deny log on as a service Description: The Deny log on as a service user right on workstations must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right. Class: compliance Tests: • false (One or more child checks must be true.) ◦ false (All child checks must be true.) ▪ false (All child checks must be true.) ▪ false (System is not a member of a domain) ◦ false (All child checks must be true.) ▪ false (Deny log on as a service - Domain Admins) ▪ false (Deny log on as a service - Enterprise Admins) ▪ true (All child checks must be true.) (negated) ▪ false (System is not a member of a domain)
Tests:	Test ID: oval:mil.disa.fso.windows:tst:498200 (wmi_test) Result: false

Title:	System is not a member of a domain
Check Existence:	One or more collected items must exist.
Check:	All collected items must match the given state(s).
State Operator:	One or more item-state comparisons may be true.
Object ID:	oval:mil.disa.fso.windows:obj:498200 (wmi_object)
Object Requirements:	• namespace must be equal to 'root\cimv2' • wql must be equal to 'SELECT DomainRole FROM win32_computersystem'
State ID:	oval:mil.disa.fso.windows:ste:498200 (wmi_state)
State Requirements:	• all result must be equal to '0'
State ID:	oval:mil.disa.fso.windows:ste:498203 (wmi_state)
State Requirements:	• all result must be equal to '2'
Collected Item Properties:	• namespace equals 'root\cimv2' • wql equals 'SELECT DomainRole FROM win32_computersystem' • result equals '1'
Additional Information:	Check requirement not met.

Test ID:	oval:mil.disa.fso.windows:tst:437400 (accesstoken_test)
Result:	false
Title:	Deny log on as a service - Domain Admins
Check Existence:	One or more collected items must exist.
Check:	At least one collected item must match the given state(s).
Object ID:	oval:mil.disa.fso.windows:obj:477500 (accesstoken_object)
Object Requirements:	• Collect any available items.
State ID:	oval:mil.disa.fso.windows:ste:437200 (accesstoken_state)
State Requirements:	• all sedenyservicelogonright must be equal to '1'
Collected Item Properties:	• Message - 'security_principle' • security_principle equals 'Domain Admins' • seassignprimarytokenprivilege equals '0' • seauditprivilege equals '0' • sebackupprivilege equals '0' • sechangenotifyprivilege equals '0' • secreateglobalprivilege equals '0' • secreatepagefileprivilege equals '0' • secreatepermanentprivilege equals '0' • secreatesymboliclinkprivilege equals '0' • secreatetokenprivilege equals '0' • sedebugprivilege equals '0' • seenabledelegationprivilege equals '0' • seimpersonateprivilege equals '0' • seincreasebasepriorityprivilege equals '0' • seincreasequotaprivilege equals '0' • seincreaseworkingsetprivilege equals '0' • seloaddriverprivilege equals '0' • selockmemoryprivilege equals '0' • semachineaccountprivilege equals '0' • semanagevolumeprivilege equals '0' • seprofilesingleprocessprivilege equals '0' • serelabelprivilege equals '0'

- seremoteshutdownprivilege equals '0'
- serestoreprivilege equals '0'
- sesecurityprivilege equals '0'
- seshutdownprivilege equals '0'
- sesyncagentprivilege equals '0'
- sesystemenvironmentprivilege equals '0'
- sesystemprofileprivilege equals '0'
- sesystemtimeprivilege equals '0'
- setakeownershipprivilege equals '0'
- setcbprivilege equals '0'
- setimezoneprivilege equals '0'
- seundockprivilege equals '0'
- seunsolicitedinputprivilege equals '0'
- sebatchlogonright equals '0'
- seinteractivelogonright equals '0'
- senetworklogonright equals '0'
- seremoteinteractivelogonright equals '0'
- seservicelogonright equals '0'
- sedenybatchLogonright equals '1'
- sedenyinteractivelogonright equals '0'
- sedenynetworklogonright equals '0'
- sedenyremoteInteractivelogonright equals '0'
- sedenyservicelogonright equals '0'
- setrustedcredmanaccessnameright equals '0'

Additional Information: Check requirement not met.

Test ID: oval:mil.disa.fso.windows:tst:437401 (accesstoken_test)
Result: false
Title: Deny log on as a service - Enterprise Admins
Check Existence: One or more collected items must exist.
Check: At least one collected item must match the given state(s).
Object ID: oval:mil.disa.fso.windows:obj:477501 (accesstoken_object)
Object Requirements:
- Collect any available items.

State ID: oval:mil.disa.fso.windows:ste:437200 (accesstoken_state)
State Requirements:
- all sedenyservicelogonright must be equal to '1'

Collected Item Properties:
- Message - 'security_principle'
- security_principle equals 'Enterprise Admins'
- seassignprimarytokenprivilege equals '0'
- seauditprivilege equals '0'
- sebackupprivilege equals '0'
- sechangenotifyprivilege equals '0'
- secreateglobalprivilege equals '0'
- secreatepagefileprivilege equals '0'
- secreatepermanentprivilege equals '0'
- secreatesymboliclinkprivilege equals '0'
- secreatetokenprivilege equals '0'
- sedebugprivilege equals '0'
- seenabledelegationprivilege equals '0'

	• seimpersonateprivilege equals '0' • seincreasebasepriorityprivilege equals '0' • seincreasequotaprivilege equals '0' • seincreaseworkingsetprivilege equals '0' • seloaddriverprivilege equals '0' • selockmemoryprivilege equals '0' • semachineaccountprivilege equals '0' • semanagevolumeprivilege equals '0' • seprofilesingleprocessprivilege equals '0' • serelabelprivilege equals '0' • seremoteshutdownprivilege equals '0' • serestoreprivilege equals '0' • sesecurityprivilege equals '0' • seshutdownprivilege equals '0' • sesyncagentprivilege equals '0' • sesystemenvironmentprivilege equals '0' • sesystemprofileprivilege equals '0' • sesystemtimeprivilege equals '0' • setakeownershipprivilege equals '0' • setcbprivilege equals '0' • setimezoneprivilege equals '0' • seundockprivilege equals '0' • seunsolicitedinputprivilege equals '0' • sebatchlogonright equals '0' • seinteractivelogonright equals '0' • senetworklogonright equals '0' • seremoteinteractivelogonright equals '0' • seservicelogonright equals '0' • sedenybatchLogonright equals '1' • sedenyinteractivelogonright equals '0' • sedenynetworklogonright equals '0' • sedenyremoteInteractivelogonright equals '0' • sedenyservicelogonright equals '0' • setrustedcredmanaccessnameright equals '0' Additional Information: Check requirement not met.

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.

Rule ID:	xccdf_mil.disa.stig_rule_SV-220971r569187_rule
Result:	Fail
Version:	WN10-UR-000085
Identities:	SV-78367

	V-63877 CCI-000213 (NIST SP 800-53: AC-3; NIST SP 800-53A: AC-3.1; NIST SP 800-53 Rev 4: AC-3)
Description:	Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities. The "Deny log on locally" right defines accounts that are prevented from logging on interactively. In an Active Directory Domain, denying logons to the Enterprise Admins and Domain Admins groups on lower trust systems helps mitigate the risk of privilege escalation from credential theft attacks, which could lead to the compromise of an entire domain. The Guests group must be assigned this right to prevent unauthenticated access. false
Fix Text:	Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> "Deny log on locally" to include the following. Domain Systems Only: Enterprise Admins Group Domain Admins Group Privileged Access Workstations (PAWs) dedicated to the management of Active Directory are exempt from denying the Enterprise Admins and Domain Admins groups. (See the Windows Privileged Access Workstation STIG for PAW requirements.) All Systems: Guests Group
Severity:	medium
Weight:	10.0
Reference:	Title: DPMS Target Windows 10 Publisher: DISA Type: DPMS Target Subject: Windows 10 Identifier: 4072
Definitions:	Definition ID: oval:mil.disa.fso.windows:def:4375 Result: false Title: UR: Deny log on locally Description: 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. Class: compliance Tests: • false (One or more child checks must be true.) ◦ false (All child checks must be true.) ▪ true (Deny log on locally - Guests) ▪ false (All child checks must be true.) ▪ false (System is not a member of a domain) ◦ false (All child checks must be true.) ▪ true (Deny log on locally - Guests) ▪ false (Deny log on locally - Domain Admins)

- false (Deny log on as a locally - Enterprise Admins)
- true (All child checks must be true.) (negated)
  - false (System is not a member of a domain)

Tests:

Test ID: oval:mil.disa.fso.windows:tst:437600 (accesstoken_test)
Result: true
Title: Deny log on locally - Guests
Check Existence: One or more collected items must exist.
Check: All collected items must match the given state(s).
Object ID: oval:mil.disa.fso.windows:obj:437001 (accesstoken_object)
Object Requirements:
- security_principle must be equal to 'Guests'

State ID: oval:mil.disa.fso.windows:ste:437500 (accesstoken_state)
State Requirements:
- all sedenyinteractivelogonright must be equal to '1'

Test ID: oval:mil.disa.fso.windows:tst:498200 (wmi_test)
Result: false
Title: System is not a member of a domain
Check Existence: One or more collected items must exist.
Check: All collected items must match the given state(s).
State Operator: One or more item-state comparisons may be true.
Object ID: oval:mil.disa.fso.windows:obj:498200 (wmi_object)
Object Requirements:
- namespace must be equal to 'root\cimv2'
- wql must be equal to 'SELECT DomainRole FROM win32_computersystem'

State ID: oval:mil.disa.fso.windows:ste:498200 (wmi_state)
State Requirements:
- all result must be equal to '0'

State ID: oval:mil.disa.fso.windows:ste:498203 (wmi_state)
State Requirements:
- all result must be equal to '2'

Collected Item Properties:
- namespace equals 'root\cimv2'
- wql equals 'SELECT DomainRole FROM win32_computersystem'
- result equals '1'

Additional Information: Check requirement not met.

Test ID: oval:mil.disa.fso.windows:tst:437700 (accesstoken_test)
Result: false
Title: Deny log on locally - Domain Admins
Check Existence: One or more collected items must exist.
Check: At least one collected item must match the given state(s).
Object ID: oval:mil.disa.fso.windows:obj:477500 (accesstoken_object)
Object Requirements:
- Collect any available items.

State ID: oval:mil.disa.fso.windows:ste:437500 (accesstoken_state)
State Requirements:
- all sedenyinteractivelogonright must be equal to '1'

Collected Item Properties:
- Message - 'security_principle'
- security_principle equals 'Domain Admins'
- seassignprimarytokenprivilege equals '0'
- seauditprivilege equals '0'
- sebackupprivilege equals '0'
- sechangenotifyprivilege equals '0'
- secreateglobalprivilege equals '0'

- secreatepagefileprivilege equals '0'
- secreatepermanentprivilege equals '0'
- secreatesymboliclinkprivilege equals '0'
- secreatetokenprivilege equals '0'
- sedebugprivilege equals '0'
- seenabledelegationprivilege equals '0'
- seimpersonateprivilege equals '0'
- seincreasebasepriorityprivilege equals '0'
- seincreasequotaprivilege equals '0'
- seincreaseworkingsetprivilege equals '0'
- seloaddriverprivilege equals '0'
- selockmemoryprivilege equals '0'
- semachineaccountprivilege equals '0'
- semanagevolumeprivilege equals '0'
- seprofilesingleprocessprivilege equals '0'
- serelabelprivilege equals '0'
- seremoteshutdownprivilege equals '0'
- serestoreprivilege equals '0'
- sesecurityprivilege equals '0'
- seshutdownprivilege equals '0'
- sesyncagentprivilege equals '0'
- sesystemenvironmentprivilege equals '0'
- sesystemprofileprivilege equals '0'
- sesystemtimeprivilege equals '0'
- setakeownershipprivilege equals '0'
- setcbprivilege equals '0'
- setimezoneprivilege equals '0'
- seundockprivilege equals '0'
- seunsolicitedinputprivilege equals '0'
- sebatchlogonright equals '0'
- seinteractivelogonright equals '0'
- senetworklogonright equals '0'
- seremoteinteractivelogonright equals '0'
- seservicelogonright equals '0'
- sedenybatchLogonright equals '1'
- sedenyinteractivelogonright equals '0'
- sedenynetworklogonright equals '0'
- sedenyremoteInteractivelogonright equals '0'
- sedenyservicelogonright equals '0'
- setrustedcredmanaccessnameright equals '0'

Additional Information: Check requirement not met.

Test ID: oval:mil.disa.fso.windows:tst:437701 (accesstoken_test)
Result: false
Title: Deny log on as a locally - Enterprise Admins
Check Existence: One or more collected items must exist.
Check: At least one collected item must match the given state(s).
Object ID: oval:mil.disa.fso.windows:obj:477501 (accesstoken_object)

Object Requirements:	• Collect any available items.
State ID:	oval:mil.disa.fso.windows:ste:437500 (accesstoken_state)
State Requirements:	• all sedenyinteractivelogonright must be equal to '1'
Collected Item Properties:	• Message - 'security_principle' • security_principle equals 'Enterprise Admins' • seassignprimarytokenprivilege equals '0' • seauditprivilege equals '0' • sebackupprivilege equals '0' • sechangenotifyprivilege equals '0' • secreateglobalprivilege equals '0' • secreatepagefileprivilege equals '0' • secreatepermanentprivilege equals '0' • secreatesymboliclinkprivilege equals '0' • secreatetokenprivilege equals '0' • sedebugprivilege equals '0' • seenabledelegationprivilege equals '0' • seimpersonateprivilege equals '0' • seincreasebasepriorityprivilege equals '0' • seincreasequotaprivilege equals '0' • seincreaseworkingsetprivilege equals '0' • seloaddriverprivilege equals '0' • selockmemoryprivilege equals '0' • semachineaccountprivilege equals '0' • semanagevolumeprivilege equals '0' • seprofilesingleprocessprivilege equals '0' • serelabelprivilege equals '0' • seremoteshutdownprivilege equals '0' • serestoreprivilege equals '0' • sesecurityprivilege equals '0' • seshutdownprivilege equals '0' • sesyncagentprivilege equals '0' • sesystemenvironmentprivilege equals '0' • sesystemprofileprivilege equals '0' • sesystemtimeprivilege equals '0' • setakeownershipprivilege equals '0' • setcbprivilege equals '0' • setimezoneprivilege equals '0' • seundockprivilege equals '0' • seunsolicitedinputprivilege equals '0' • sebatchlogonright equals '0' • seinteractivelogonright equals '0' • senetworklogonright equals '0' • seremoteinteractivelogonright equals '0' • seservicelogonright equals '0' • sedenybatchLogonright equals '1' • sedenyinteractivelogonright equals '0' • sedenynetworklogonright equals '0' • sedenyremoteInteractivelogonright equals '0'

	• sedenyservicelogonright equals '0' • setrustedcredmanaccessnameright equals '0' Additional Information: Check requirement not met.