

The screenshot shows a Microsoft Word document titled "CIS\_Microsoft\_Windows\_Server\_2016\_RTM\_Release\_1607\_Benchmark\_v1.1.0.pdf". The document is displayed in a browser window at the URL [199.188.127.130](http://199.188.127.130).

**18.9.28 Event Viewer**

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `EventViewer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

**18.9.29 Family Safety (formerly Parental Controls)**

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `ParentalControls.admx/adml` that is only included with the Microsoft Windows Vista through the Windows 10 RTM (Release 1507) Administrative Templates.

**Note:** This section was initially named *Parental Controls* but was renamed by Microsoft to *Family Safety* starting with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

**18.9.30 File Explorer (formerly Windows Explorer)**

**18.9.26.4.2 (L1) Ensure 'System: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (Scored)**

**Profile Applicability:**

- Level 1 - Domain Controller
- Level 1 - Member Server

**Description:**

This policy setting specifies the maximum size of the log file in kilobytes. The maximum log file size can be configured between 1 megabyte (1,024 kilobytes) and 4 terabytes (4,194,240 kilobytes) in kilobyte increments.

The recommended state for this setting is: Enabled: 32,768 or greater.

**Rationale:**

If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users

**Audit:**

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\EventLog\System:MaxSize

**Remediation:**

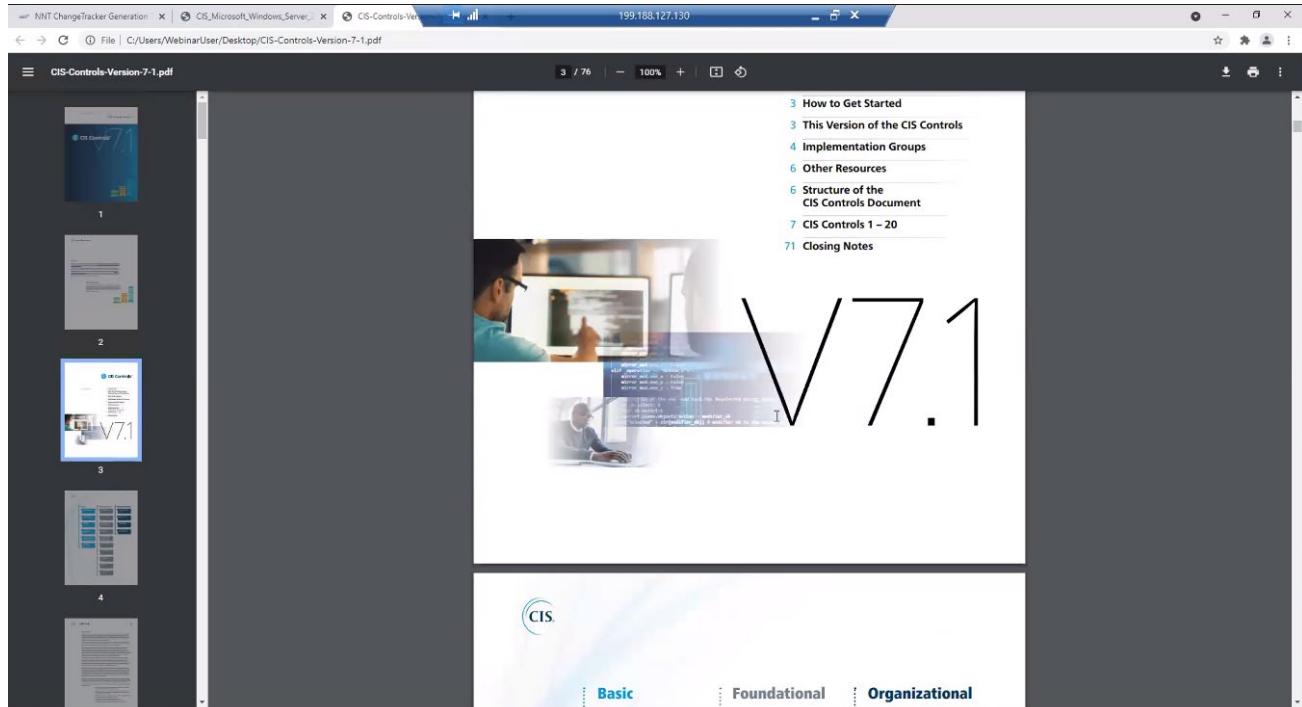
To establish the recommended configuration via GP, set the following UI path to Enabled: 32,768 or greater:

Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\System\Specify the maximum log file size (KB)

**Note:** This Group Policy path is provided by the Group Policy template EventLog.admx/adml that is included with all versions of the Microsoft Windows Administrative Templates.  
**Note #2:** In older Microsoft Windows Administrative Templates, this setting was initially named *Maximum Log Size (KB)*, but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

687 | Page

## CIS Controls v7.1



The screenshot shows a PDF document titled "CIS-Controls-Version-7-1.pdf" open in a web browser. The page number is 3 / 76. The document contains several sections and images. On the left, there's a vertical sidebar with four numbered icons: 1 (blue square), 2 (grey square), 3 (blue square), and 4 (grey square). The main content area features a large image of two people working at a computer. To the right of the image is a vertical navigation menu with the following items: 3 How to Get Started, 3 This Version of the CIS Controls, 4 Implementation Groups, 6 Other Resources, 6 Structure of the CIS Controls Document, 7 CIS Controls 1 – 20, and 71 Closing Notes. At the bottom of the page, there are three tabs: Basic, Foundational, and Organizational. The Organizational tab is highlighted.

NNT

Dashboard Events Devices ✓ Compliance Planned Changes Reports Settings

America/New\_York Admin

Compliance

Group/Device: No Selection Date/Time: Past Hour

Windows 2016 / NNT CIS Microsoft Windows Server 2016 Benchmark - Level 1 Member Server

Report Version : 1.0.0 Average Score : 65.4 % Run Time : 24 Jun 2021 09:58:09

Total Device Count : 2 Devices whose scores went up : 0 Devices that were unchanged : 2 Devices whose scores went down : 0

Data in this panel reflects the most recent run.

Device Name	24 Jun 2021 10:56:50	24 Jun 2021 10:56:54						
CIS-WRK-SHP-2	<input type="checkbox"/> 97.8 % <span style="color:red;">!</span>	<input type="checkbox"/> 97.8 % <span style="color:red;">!</span>	-	-	-	-	-	-
CIS-WRK-SHP-4	<input type="checkbox"/> 33.0 % <span style="color:red;">!</span>	<input type="checkbox"/> 33.0 % <span style="color:red;">!</span>	-	-	-	-	-	-

1 - 2 of 2 items

Audio Settings ^ Chat Raise Hand Q&A Leave

Change Details

Rule Title	CIS-WRK-SHP-2	CIS-WRK-SHP-4	Reason for change
2.2.21 (L1) Ensure 'Deny log on through Remote Desktop Services' to include 'Guests, Local account'	✓	✗	FAILED: (L1) Ensure 'Deny log on through Remote Desktop Services' to include 'Guests, Local account' : securitypolicy (.). Remediation : To establish the recommended configuration via GP, set the following UI path to include Guests, Local account:Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Deny log on through Remote Desktop Services Impact: If you assign the Deny log on through Terminal Services user right to other groups, you could limit the abilities of users who are assigned to specific administrative roles in your environment. Accounts that have this user right will be unable to connect to the computer through either Terminal Services or Remote Assistance. You should confirm that delegated tasks will not be negatively impacted.
2.2.37 (L1) Ensure 'Restore files and directories' is set to 'Administrators'	✓	✗	FAILED: (L1) Ensure 'Restore files and directories' is set to 'Administrators' : securitypolicy (BUILTIN\BACKUP OPERATORS). Remediation : To establish the recommended configuration via GP, set the following UI path to Administrators:Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Restore files and directories Impact: If you remove the Restore files and directories user right from the Backup Operators group and other accounts you could make it impossible for users who have been delegated specific tasks to perform those tasks. You should verify that this change won't negatively affect the ability of your organization's personnel to do their jobs.
			FAILED: (L1) Ensure 'Shut down the system' is set to 'Administrators' : securitypolicy (BUILTIN\OPERATORS). Remediation : To establish the recommended configuration via GP, set the following UI path to Administrators:Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Shut down the system Impact: If you remove the Shut down the system user right from the Operators group and other accounts you could make it impossible for users who have been delegated specific tasks to perform those tasks. You should verify that this change won't negatively affect the ability of your organization's personnel to do their jobs.

## Account Lockout Policy

### Account Policies Rules

1.2.1 (L1) Ensure 'Account lockout duration' is set to '15 or more minute(s)'

Pass

Pass: PASSED: '15'.

1.2.2 (L1) Ensure 'Account lockout threshold' is set to '10 or fewer invalid logon attempt(s), but not 0'

Pass

Pass: PASSED: '5'.

1.2.3 (L1) Ensure 'Reset account lockout counter after' is set to '15 or more minute(s)'

Pass

Pass: PASSED: '15'.

## Local Policies

### User Rights Assignment

#### Local Policies Rules

2.2.1 (L1) Ensure 'Access Credential Manager as a trusted caller' is set to 'No One'

Pass

Pass: PASSED: securitypolicy () .

2.2.2 (L1) Configure 'Access this computer from the network'

Pass

Pass: PASSED: securitypolicy (2 items: NT AUTHORITY\AUTHENTICATED USERS, BUILTIN\Administrators).

2.2.3 (L1) Ensure 'Act as part of the operating system' is set to 'No One'

Pass

Pass: PASSED: ..

2.2.5 (L1) Ensure 'Adjust memory quotas for a process' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE'

Pass

Pass: PASSED: securitypolicy (3 items: NT AUTHORITY\LOCAL SERVICE, NT AUTHORITY\NETWORK SERVICE, BUILTIN\Administrators).

2.2.6 (L1) Configure 'Allow log on locally'

Pass

## Reports and Queries

Group/Device: No Selection

Reports Output

Report or Query Name	Owner	Action Buttons
Windows 2016 / NNT CIS Microsoft Windows Server 2016 Benchmark - Level 1 Member Server	admin	<a href="#">Run</a> <a href="#">Edit</a>
Previous runs of this report are shown below. Preview or download them using layout template: <a href="#">Compliance Detail</a>		
24 Jun 09:56:54 ✓ Windows 2016 / NNT CIS Microsoft Windows Server 2016 Benchmark - Level 1 Member Server: 2 reports	Results available until 25 Jun 09:56:54	<a href="#">Preview</a> <a href="#">Options</a> <a href="#">Download</a> <a href="#">Delete</a>
24 Jun 09:56:50 ✓ Windows 2016 / NNT CIS Microsoft Windows Server 2016 Benchmark - Level 1 Member Server: 2 reports	Results available until 25 Jun 09:56:50	<a href="#">Preview</a> <a href="#">Options</a> <a href="#">Download</a> <a href="#">Delete</a>
23 Jun 22:34:18 ✓ Windows 2016 / NNT CIS Microsoft Windows Server 2016 Benchmark - Level 1 Member Server: 2 reports	Results available until 24 Jun 22:34:18	<a href="#">Preview</a> <a href="#">Options</a> <a href="#">Download</a> <a href="#">Delete</a>
Windows 2016 Remediation / NNT Remediated CIS Microsoft Windows Server 2016 Benchmark - Level 1 Member Server	admin	<a href="#">Run</a> <a href="#">Edit</a>
Previous runs of this report are shown below. Preview or download them using layout template: <a href="#">Compliance Detail</a>		
24 Jun 09:56:55 ✓ Windows 2016 Remediation / NNT Remediated CIS Microsoft Windows Server 2016 Benchmark - Level 1 Member Server: 2 reports	Results available until 25 Jun 09:56:55	<a href="#">Preview</a> <a href="#">Options</a> <a href="#">Download</a> <a href="#">Delete</a>
24 Jun 09:56:53 ✓ Windows 2016 Remediation / NNT Remediated CIS Microsoft Windows Server 2016 Benchmark - Level 1 Member Server: 2 reports	Results available until 25 Jun 09:56:53	<a href="#">Preview</a> <a href="#">Options</a> <a href="#">Download</a> <a href="#">Delete</a>
23 Jun 22:34:17 ✓ Windows 2016 Remediation / NNT Remediated CIS Microsoft Windows Server 2016 Benchmark - Level 1 Member Server: 2 reports	Results available until 24 Jun 22:34:17	<a href="#">Preview</a> <a href="#">Options</a> <a href="#">Download</a> <a href="#">Delete</a>

1 - 3 of 3 items

NNT ChangeTracker Generation x CIS\_Microsoft\_Windows\_Server\_... x CIS-Controls-Ven... 199.188.127.130

File | C:/Users/WebinarUser/Desktop/Evaluation%20preadsheet%20-%20Windows%202016%20\_%20NNT%20CIS%20Microsoft%20Windows%20Server%20Benchmark%20-%20Level%201%20Member%20Server.xlsx

Evaluation Spreadsheet - Windows 2016 \_ NNT CIS Microsoft Windows Server 2016 Benchmark - Level 1 Member Server.xlsx

File Edit Insert Format Help Download Share

Windows 2016 / NNT CIS Microsoft Windows Server 2016 Benchmark - Level 1 Member Server

COLOR KEY:  
 Green = Alter Setting w/o Evaluation  
 Yellow = Setting Requires Evaluation  
 Grey = Setting Does Not Apply

**Settings**

Run User Name: admin Run Started by: User  
 Report Run Date: 22 Oct 2019 Time Zone: Europe/London  
 Previous Report Run Date: 17 Oct 2019 Compliance Report Version: 1.0.0

**CIS-WRK-SHP-4**  
 CIS Microsoft Windows Server 2016 Benchmark - Level 1 Member Server

This document provides prescriptive guidance for establishing a secure configuration posture for Microsoft Windows Server. To obtain the latest version of this guide, please visit <http://benchmarks.cisecurity.org>. If you have questions, comments, or have identified ways to improve this guide, please write us at [feedback@cisecurity.org](mailto:feedback@cisecurity.org).

**Total Score 32.97% (Previous: 32.97 %)**

**Account Policies**

**Password Policy**

**Account Policies Rules**

1.1.1 (L1) Ensure 'Enforce password history' is set to '24 or more password(s)'  
 Fail: FAILED: (L1) Ensure 'Enforce password history' is set to '24 or more password(s)'. Remediation: To establish the recommended configuration via GP, set the following UI path to 24 or more password(s) Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Accounts:Enforce password history Impact: The major impact of this configuration is that users must create a new password every time they are required to change their old one. If users are required to change their passwords to new unique values, there is an increased risk of users who write their passwords somewhere so that they do not forget them. Another risk is that users may create passwords that change incrementally (for example, password01, password02, and so on) to facilitate memorization but makes them easier to guess. Also, an unnecessary burden for the business.

Page 1

Audio Settings ^ Chat Raise Hand Q&A Leave

161 2.3.1.6 (L1) Configure 'Accounts: Rename guest account'  
 Fail: FAILED: (L1) Configure 'Accounts: Rename guest account' : "Guest". Remediation: To establish the recommended configuration via GP, configure the following UI path: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Rename guest account Impact: You will have to inform users who are authorized to use this account of the new account name. (The guidance for this setting assumes that the Administrator account was not disabled, which was recommended earlier in this chapter.).

163 2.3.1.6 (L1) Configure 'Accounts: Rename guest account'  
 Fail - Alter Setting

165 Fail: FAILED: (L1) Configure 'Accounts: Rename guest account' : "Guest". Remediation: To establish the recommended configuration via GP, configure the following UI path: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Rename guest account Impact: There should be little impact, because the Guest account is disabled by default.

168

169 **Audit Rules**

2.3.2.1 (L1) Ensure 'Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings' is set to 'Enabled'  
 Fail - Alter Setting

171 Fail: FAILED: (L1) Ensure 'Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings' is set to 'Enabled' : "...". Remediation: To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings Impact: None - this is the default configuration.

177 **Devices Rules**

2.3.4.1 (L1) Ensure 'Devices: Allowed to format and eject removable media' is set to 'Administrators'  
 Fail - Alter Setting

179 Fail: FAILED: (L1) Ensure 'Devices: Allowed to format and eject removable media' is set to 'Administrators' : "...". Remediation: To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Devices: Allowed to format and eject removable media Impact: None - this is the default configuration.

185 **Interactive logon Rules**

2.3.7.1 (L1) Ensure 'Interactive logon: Do not display last user name' is set to 'Enabled'  
 Fail - Alter Setting

187 Fail: FAILED: (L1) Ensure 'Interactive logon: Do not display last user name' is set to 'Enabled' : '0'. Remediation: To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Do not display last user name Impact: The name of the last user to successfully log on is not be displayed in the Windows logon screen.

189 2.3.7.3 (L1) Ensure 'Interactive logon: Machine inactivity limit' is set to '900 or fewer second(s), but not 0'  
 Fail - Alter Setting

191 Fail: FAILED: (L1) Ensure 'Interactive logon: Machine inactivity limit' is set to '900 or fewer second(s), but not 0' :

setting to reduce help desk calls. Note: With this setting configured as recommended, the default error message displayed when a user attempts to perform an operation or run a program requiring privilege elevation (without Administrator rights) is "This program will not run. This program is blocked by group policy. For more information, contact your system administrator." Some users who are not used to seeing this message may believe that the operation or program they attempted is specifically blocked by group policy, as that is what the message seems to imply. This message may therefore result in user questions as to why that specific operation/program is blocked, when in fact, the problem is that they need to perform the operation or run the program with an Administrative account (or "Run as Administrator" if it is already an Administrator account), and they are not doing that.

345	<b>Windows Firewall With Advanced Security</b>
346	<b>Domain Profile</b>
347	<b>Windows Firewall With Advanced Security Rules</b>
350	9.1.1 (L1) Ensure 'Windows Firewall: Domain: Firewall state' is set to 'On (recommended)'
352	<b>Fail - Setting Does Not Apply - Utilizing 3rd Party Tool</b>
354	Fail: FAILED: (L1) Ensure 'Windows Firewall: Domain: Firewall state' is set to 'On (recommended)' : ". Remediation : To establish the recommended configuration via GP, set the following UI path to On (recommended) Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Firewall state Impact:None - this is the default configuration.
356	9.1.2 (L1) Ensure 'Windows Firewall: Domain: Inbound connections' is set to 'Block (default)'
358	<b>Fail - Setting Does Not Apply - Utilizing 3rd Party Tool</b>
360	Fail: FAILED: (L1) Ensure 'Windows Firewall: Domain: Inbound connections' is set to 'Block (default)' : ". Remediation : To establish the recommended configuration via GP, set the following UI path to Block (default) Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Inbound connections Impact:None - this is the default configuration.
362	9.1.3 (L1) Ensure 'Windows Firewall: Domain: Outbound connections' is set to 'Allow (default)'
364	<b>Fail - Setting Does Not Apply - Utilizing 3rd Party Tool</b>
365	Fail: FAILED: (L1) Ensure 'Windows Firewall: Domain: Outbound connections' is set to 'Allow (default)' : ". Remediation : To establish the recommended configuration via GP, set the following UI path to Allow (default) Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Outbound connections Impact:None - this is the default configuration.
369	9.1.4 (L1) Ensure 'Windows Firewall: Domain: Settings: Display a notification' is set to 'No' (CCE Reference : CCE-38041-0)
371	<b>Fail - Setting Does Not Apply - Utilizing 3rd Party Tool</b>
372	Fail: FAILED: (L1) Ensure 'Windows Firewall: Domain: Settings: Display a notification' is set to 'No' : ". Remediation : To establish the recommended configuration via GP, set the following UI path to No:Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Settings\Customize\Display a

Page 1

## Remediation kit

```

C:\Users\WebinarUser\Desktop\NNT Remediated CIS Microsoft Windows Server 2016 Benchmark - Level 1 Member Server.xml 199.188.127.130
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ? X

NNT Remediated CIS Microsoft Windows Server 2016 Benchmark - Level 1 Member Server.xml [ NNT CIS Red Hat Enterprise Linux 7 Server Benchmark - Level 1.xml ]
2951 <RuleExpression Value="1" />
2952 </InputValue>
2953 <Rule>((oval:org.cisecurity.benchmarks.microsoft_windows_server_2016:obj:10239) == (oval:org.cisecurity.benchmarks.microsoft_windows_server_2016:ste:10132))</Rule> FailuresExpression="FAILED: (L1) Ensure 'Use
2954 <OperatingSystems>
2955 <OperatingSystem>All</OperatingSystem>
2956 </OperatingSystems>
2957 <RuleExpression>
2958 </Rule>
2959 <SubCategory>
2960 <Category>Domain Profile</Category>
2961 <Section Name="Windows Firewall With Advanced Security">
2962 <Category>Domain Profile</Category>
2963 <SubCategory Name="Windows Firewall With Advanced Security Rules">
2964 <Rule Number="9.1.1" Name="Remediated - (L1) Ensure 'Windows Firewall: Domain: Firewall state' is set to 'On (recommended)'>
2965 <Description>Description: Select On (recommended) to have Windows Firewall with Advanced Security use the settings for this profile to filter network traffic. If you select Off, Windows Firewall with Advanced Security
2966 <RuleExpression Rule="1==1" ShowFailureExpression="Never" FailuresExpression="" ShowPassesExpression="WhenRulePasses" PassesExpression="Note: this test is not automatically evaluated. The rule has been deemed not suit
2967 <OperatingSystems>
2968 <OperatingSystem>All</OperatingSystem>
2969 </OperatingSystems>
2970 </RuleExpressions>
2971 <ResultText GeneralPreamble="Note: this test is not automatically evaluated. The rule has been deemed not suitable for the environment." ShowGeneralPreamble="Always" />
2972 <Rule Number="9.1.2" Name="Remediated - (L1) Ensure 'Windows Firewall: Domain: Inbound connections' is set to 'Block (default)'>
2973 <Description>Description: This setting determines the behavior for inbound connections that do not match an inbound firewall rule. The recommended state for this setting is: Block (default). Rationale: If the firewall a
2974 <RuleExpression Rule="1==1" ShowFailureExpression="Never" FailuresExpression="" ShowPassesExpression="WhenRulePasses" PassesExpression="Note: this test is not automatically evaluated. The rule has been deemed not suit
2975 <OperatingSystems>
2976 <OperatingSystem>All</OperatingSystem>
2977 </OperatingSystems>
2978 </RuleExpression>
2979 <ResultText GeneralPreamble="Note: this test is not automatically evaluated. The rule has been deemed not suitable for the environment." ShowGeneralPreamble="Always" />
2980 <Rule Number="9.1.3" Name="Remediated - (L1) Ensure 'Windows Firewall: Domain: Outbound connections' is set to 'Allow (default)'>
2981 <Description>Description: This setting determines the behavior for outbound connections that do not match an outbound firewall rule. The recommended state for this setting is: Allow (default). Rationale: Some people bel
2982 <RuleExpression Rule="1==1" ShowFailureExpression="Never" FailuresExpression="" ShowPassesExpression="WhenRulePasses" PassesExpression="Note: this test is not automatically evaluated. The rule has been deemed not suit
2983 <OperatingSystems>
2984 <OperatingSystem>All</OperatingSystem>
2985 </OperatingSystems>
2986 </RuleExpression>
2987 <ResultText GeneralPreamble="Note: this test is not automatically evaluated. The rule has been deemed not suitable for the environment." ShowGeneralPreamble="Always" />
2988 <Rule Number="9.1.4" Name="Remediated - (L1) Ensure 'Windows Firewall: Domain: Settings: Display a notification' is set to 'No' (CCE Reference : CCE-38041-0)">
2989 <Description>Description: Select this option to have Windows Firewall with Advanced Security display notifications to the user when a program is blocked from receiving inbound connections. The recommended state for this
2990 <RuleExpression Rule="1==1" ShowFailureExpression="Never" FailuresExpression="" ShowPassesExpression="WhenRulePasses" PassesExpression="Note: this test is not automatically evaluated. The rule has been deemed not suit
2991 <OperatingSystems>
2992 <OperatingSystem>All</OperatingSystem>
2993 </OperatingSystems>
2994 </RuleExpression>
2995 <ResultText GeneralPreamble="Note: this test is not automatically evaluated. The rule has been deemed not suitable for the environment." ShowGeneralPreamble="Always" />
2996 <Rule Number="9.1.5" Name="Remediated - (L1) Ensure 'Windows Firewall: Domain: Settings: Apply local firewall rules' is set to 'Yes (default)'>
2997 <Description>Description: This setting controls whether local administrators are allowed to create local firewall rules that apply together with firewall rules configured by Group Policy. The recommended state for this
2998 <RuleExpression Rule="1==1" ShowFailureExpression="Never" FailuresExpression="" ShowPassesExpression="WhenRulePasses" PassesExpression="Note: this test is not automatically evaluated. The rule has been deemed not suit
2999 </Rule>
3000 </RuleExpressions>
3001 </Rule>
3002 </Rule>
3003 </Rule>
3004 </Rule>
3005 </Rule>
3006 </Rule>
3007 </Rule>
3008 </Rule>
3009 </Rule>
3010 </Rule>
3011 </Rule>
3012 </Rule>
3013 </Rule>
3014 </Rule>
3015 </Rule>
3016 </Rule>
3017 </Rule>
3018 </Rule>
3019 </Rule>
3020 </Rule>
3021 </Rule>
3022 </Rule>
3023 </Rule>
3024 </Rule>
3025 </Rule>
3026 </Rule>
3027 </Rule>
3028 </Rule>
3029 </Rule>
3030 </Rule>
3031 </Rule>
3032 </Rule>
3033 </Rule>
3034 </Rule>
3035 </Rule>
3036 </Rule>
3037 </Rule>
3038 </Rule>
3039 </Rule>
3040 </Rule>
3041 </Rule>
3042 </Rule>
3043 </Rule>
3044 </Rule>
3045 </Rule>
3046 </Rule>
3047 </Rule>
3048 </Rule>
3049 </Rule>
3050 </Rule>
3051 </Rule>
3052 </Rule>
3053 </Rule>
3054 </Rule>
3055 </Rule>
3056 </Rule>
3057 </Rule>
3058 </Rule>
3059 </Rule>
3060 </Rule>
3061 </Rule>
3062 </Rule>
3063 </Rule>
3064 </Rule>
3065 </Rule>
3066 </Rule>
3067 </Rule>
3068 </Rule>
3069 </Rule>
3070 </Rule>
3071 </Rule>
3072 </Rule>
3073 </Rule>
3074 </Rule>
3075 </Rule>
3076 </Rule>
3077 </Rule>
3078 </Rule>
3079 </Rule>
3080 </Rule>
3081 </Rule>
3082 </Rule>
3083 </Rule>
3084 </Rule>
3085 </Rule>
3086 </Rule>
3087 </Rule>
3088 </Rule>
3089 </Rule>
3090 </Rule>
3091 </Rule>
3092 </Rule>
3093 </Rule>
3094 </Rule>
3095 </Rule>
3096 </Rule>
3097 </Rule>
3098 </Rule>
3099 </Rule>
3100 </Rule>
3101 </Rule>
3102 </Rule>
3103 </Rule>
3104 </Rule>
3105 </Rule>
3106 </Rule>
3107 </Rule>
3108 </Rule>
3109 </Rule>
3110 </Rule>
3111 </Rule>
3112 </Rule>
3113 </Rule>
3114 </Rule>
3115 </Rule>
3116 </Rule>
3117 </Rule>
3118 </Rule>
3119 </Rule>
3120 </Rule>
3121 </Rule>
3122 </Rule>
3123 </Rule>
3124 </Rule>
3125 </Rule>
3126 </Rule>
3127 </Rule>
3128 </Rule>
3129 </Rule>
3130 </Rule>
3131 </Rule>
3132 </Rule>
3133 </Rule>
3134 </Rule>
3135 </Rule>
3136 </Rule>
3137 </Rule>
3138 </Rule>
3139 </Rule>
3140 </Rule>
3141 </Rule>
3142 </Rule>
3143 </Rule>
3144 </Rule>
3145 </Rule>
3146 </Rule>
3147 </Rule>
3148 </Rule>
3149 </Rule>
3150 </Rule>
3151 </Rule>
3152 </Rule>
3153 </Rule>
3154 </Rule>
3155 </Rule>
3156 </Rule>
3157 </Rule>
3158 </Rule>
3159 </Rule>
3160 </Rule>
3161 </Rule>
3162 </Rule>
3163 </Rule>
3164 </Rule>
3165 </Rule>
3166 </Rule>
3167 </Rule>
3168 </Rule>
3169 </Rule>
3170 </Rule>
3171 </Rule>
3172 </Rule>
3173 </Rule>
3174 </Rule>
3175 </Rule>
3176 </Rule>
3177 </Rule>
3178 </Rule>
3179 </Rule>
3180 </Rule>
3181 </Rule>
3182 </Rule>
3183 </Rule>
3184 </Rule>
3185 </Rule>
3186 </Rule>
3187 </Rule>
3188 </Rule>
3189 </Rule>
3190 </Rule>
3191 </Rule>
3192 </Rule>
3193 </Rule>
3194 </Rule>
3195 </Rule>
3196 </Rule>
3197 </Rule>
3198 </Rule>
3199 </Rule>
3200 </Rule>
3201 </Rule>
3202 </Rule>
3203 </Rule>
3204 </Rule>
3205 </Rule>
3206 </Rule>
3207 </Rule>
3208 </Rule>
3209 </Rule>
3210 </Rule>
3211 </Rule>
3212 </Rule>
3213 </Rule>
3214 </Rule>
3215 </Rule>
3216 </Rule>
3217 </Rule>
3218 </Rule>
3219 </Rule>
3220 </Rule>
3221 </Rule>
3222 </Rule>
3223 </Rule>
3224 </Rule>
3225 </Rule>
3226 </Rule>
3227 </Rule>
3228 </Rule>
3229 </Rule>
3230 </Rule>
3231 </Rule>
3232 </Rule>
3233 </Rule>
3234 </Rule>
3235 </Rule>
3236 </Rule>
3237 </Rule>
3238 </Rule>
3239 </Rule>
3240 </Rule>
3241 </Rule>
3242 </Rule>
3243 </Rule>
3244 </Rule>
3245 </Rule>
3246 </Rule>
3247 </Rule>
3248 </Rule>
3249 </Rule>
3250 </Rule>
3251 </Rule>
3252 </Rule>
3253 </Rule>
3254 </Rule>
3255 </Rule>
3256 </Rule>
3257 </Rule>
3258 </Rule>
3259 </Rule>
3260 </Rule>
3261 </Rule>
3262 </Rule>
3263 </Rule>
3264 </Rule>
3265 </Rule>
3266 </Rule>
3267 </Rule>
3268 </Rule>
3269 </Rule>
3270 </Rule>
3271 </Rule>
3272 </Rule>
3273 </Rule>
3274 </Rule>
3275 </Rule>
3276 </Rule>
3277 </Rule>
3278 </Rule>
3279 </Rule>
3280 </Rule>
3281 </Rule>
3282 </Rule>
3283 </Rule>
3284 </Rule>
3285 </Rule>
3286 </Rule>
3287 </Rule>
3288 </Rule>
3289 </Rule>
3290 </Rule>
3291 </Rule>
3292 </Rule>
3293 </Rule>
3294 </Rule>
3295 </Rule>
3296 </Rule>
3297 </Rule>
3298 </Rule>
3299 </Rule>
3300 </Rule>
3301 </Rule>
3302 </Rule>
3303 </Rule>
3304 </Rule>
3305 </Rule>
3306 </Rule>
3307 </Rule>
3308 </Rule>
3309 </Rule>
3310 </Rule>
3311 </Rule>
3312 </Rule>
3313 </Rule>
3314 </Rule>
3315 </Rule>
3316 </Rule>
3317 </Rule>
3318 </Rule>
3319 </Rule>
3320 </Rule>
3321 </Rule>
3322 </Rule>
3323 </Rule>
3324 </Rule>
3325 </Rule>
3326 </Rule>
3327 </Rule>
3328 </Rule>
3329 </Rule>
3330 </Rule>
3331 </Rule>
3332 </Rule>
3333 </Rule>
3334 </Rule>
3335 </Rule>
3336 </Rule>
3337 </Rule>
3338 </Rule>
3339 </Rule>
3340 </Rule>
3341 </Rule>
3342 </Rule>
3343 </Rule>
3344 </Rule>
3345 </Rule>
3346 </Rule>
3347 </Rule>
3348 </Rule>
3349 </Rule>
3350 </Rule>
3351 </Rule>
3352 </Rule>
3353 </Rule>
3354 </Rule>
3355 </Rule>
3356 </Rule>
3357 </Rule>
3358 </Rule>
3359 </Rule>
3360 </Rule>
3361 </Rule>
3362 </Rule>
3363 </Rule>
3364 </Rule>
3365 </Rule>
3366 </Rule>
3367 </Rule>
3368 </Rule>
3369 </Rule>
3370 </Rule>
3371 </Rule>
3372 </Rule>
3373 </Rule>
3374 </Rule>
3375 </Rule>
3376 </Rule>
3377 </Rule>
3378 </Rule>
3379 </Rule>
3380 </Rule>
3381 </Rule>
3382 </Rule>
3383 </Rule>
3384 </Rule>
3385 </Rule>
3386 </Rule>
3387 </Rule>
3388 </Rule>
3389 </Rule>
3390 </Rule>
3391 </Rule>
3392 </Rule>
3393 </Rule>
3394 </Rule>
3395 </Rule>
3396 </Rule>
3397 </Rule>
3398 </Rule>
3399 </Rule>
3400 </Rule>
3401 </Rule>
3402 </Rule>
3403 </Rule>
3404 </Rule>
3405 </Rule>
3406 </Rule>
3407 </Rule>
3408 </Rule>
3409 </Rule>
3410 </Rule>
3411 </Rule>
3412 </Rule>
3413 </Rule>
3414 </Rule>
3415 </Rule>
3416 </Rule>
3417 </Rule>
3418 </Rule>
3419 </Rule>
3420 </Rule>
3421 </Rule>
3422 </Rule>
3423 </Rule>
3424 </Rule>
3425 </Rule>
3426 </Rule>
3427 </Rule>
3428 </Rule>
3429 </Rule>
3430 </Rule>
3431 </Rule>
```

length: 812,022 lines: 4,856 Ln:2,111 Col:28 Sel: 389 | 5 Unix (LF) UTF-8 INS

C:\Users\WebinarUser\Desktop\NNT CIS Red Hat Enterprise Linux 7 Server Benchmark - Level 1.sh - Notepad+ - 199.188.127.130

```

1 #!/bin/bash
2 PROFILE=$1-`Level 1 - Server`
3
4 if [ "$PROFILE" = "Level 1 - Server" ] || [ "$PROFILE" = "Level 2 - Server" ]; then
5   echo \*\*\*\* Executing Level 1 - Server profile remediation
6
7 # Ensure mounting of cramfs filesystems is disabled
8 echo
9 echo \*\*\*\* Ensure\ mounting\ of\ cramfs\ filesystems\ is\ disabled
10 modprobe -n -v cramfs | grep "install /bin/true\$" || echo "install cramfs /bin/true" >> /etc/modprobe.d/CIS.conf
11 lsmod | egrep "\*cramfs\$" && rmmod cramfs
12
13 # Ensure mounting of freevxfs filesystems is disabled
14 echo
15 echo \*\*\*\* Ensure\ mounting\ of\ freevxfs\ filesystems\ is\ disabled
16 modprobe -n -v freevxfs | grep "install /bin/true\$" || echo "install freevxfs /bin/true" >> /etc/modprobe.d/CIS.conf
17 lsmod | egrep "\*freevxfs\$" && rmmod freevxfs
18
19 # Ensure mounting of jffs2 filesystems is disabled
20 echo
21 echo \*\*\*\* Ensure\ mounting\ of\ jffs2\ filesystems\ is\ disabled
22 modprobe -n -v jffs2 | grep "install /bin/true\$" || echo "install jffs2 /bin/true" >> /etc/modprobe.d/CIS.conf
23 lsmod | egrep "\*jffs2\$" && rmmod jffs2
24
25 # Ensure mounting of hfs filesystems is disabled
26 echo
27 echo \*\*\*\* Ensure\ mounting\ of\ hfs\ filesystems\ is\ disabled
28 modprobe -n -v hfs | grep "install /bin/true\$" || echo "install hfs /bin/true" >> /etc/modprobe.d/CIS.conf
29 lsmod | egrep "\*hfs\$" && rmmod hfs
30
31 # Ensure mounting of hfsplus filesystems is disabled
32 echo
33 echo \*\*\*\* Ensure\ mounting\ of\ hfsplus\ filesystems\ is\ disabled
34 modprobe -n -v hfsplus | grep "install /bin/true\$" || echo "install hfsplus /bin/true" >> /etc/modprobe.d/CIS.conf
35 lsmod | egrep "\*hfsplus\$" && rmmod hfsplus
36
37 # Ensure mounting of squashfs filesystems is disabled
38 echo
39 echo \*\*\*\* Ensure\ mounting\ of\ squashfs\ filesystems\ is\ disabled
40 modprobe -n -v squashfs | grep "install /bin/true\$" || echo "install squashfs /bin/true" >> /etc/modprobe.d/CIS.conf
41 lsmod | egrep "\*squashfs\$" && rmmod squashfs
42
43 # Ensure mounting of udf filesystems is disabled
44 echo
45 echo \*\*\*\* Ensure\ mounting\ of\ udf\ filesystems\ is\ disabled
46 modprobe -n -v udf | grep "install /bin/true\$" || echo "install udf /bin/true" >> /etc/modprobe.d/CIS.conf
47 lsmod | egrep "\*udf\$" && rmmod udf
48
49 # Ensure mounting of FAT filesystems is disabled
50 echo
51 echo \*\*\*\* Ensure\ mounting\ of\ FAT\ filesystems\ is\ disabled
52 modprobe -n -v vfat | grep "install /bin/true\$" || echo "install vfat /bin/true" >> /etc/modprobe.d/CIS.conf
53 lsmod | egrep "\*vfat\$" && rmmod vfat
54
55 # Ensure nodev option set on /tmp partition
56 echo

```

length : 137,351 lines : 2,252 Ln :

## Workshop

REMEDIATION KIT

File Home Share View

2016 Demo 1.2 > REMEDIATION KIT >

Name	Date modified	Type	Size
DomainSyvol	10/17/2019 6:45 AM	File folder	
Backup\greport.xml	10/17/2019 7:45 AM	XML Document	8 KB
greport.xml	10/17/2019 7:45 AM	XML Document	321 KB

C:\Users\sgoskoli\Desktop\2016 Demo 1.2\Remediation Script.bat - Notepad++

File Edit Search View Encoding Language Settings Tools Macro Run Window ?

Recording

NNT ChangeTracker Generation | CIS\_Microsoft\_Windows\_Server\_2016 | CS-Controls-Venture 199.188.127.130

Not secure | 10.5.66.37/#dashboard

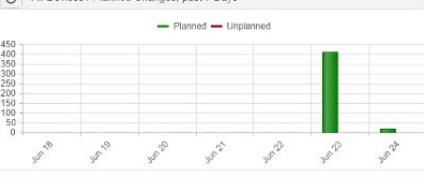
**Dashboard** Events Devices Compliance Planned Changes Reports Settings America/New\_York Admin 10:01:10 7.3.1.21 (9478)

**Dashboard** CIS Workshop Dashboard

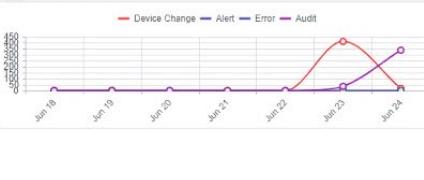
**Compliance Results (All Devices)**  
 23 Jun 2021 22:34:16 Windows 2016 (2 Devices)  
 NNT CIS Microsoft Windows Server 2016 Benchmark - Level 1 Member Server  
 23 Jun 2021 22:34:17 Windows 2016 Remediation (2 Devices)  
 NNT Remediated CIS Microsoft Windows Server 2016 Benchmark - Level 1 Member Server

**Event Stream (All Devices)**  
 Device Change Alert Error Audit  


**Devices Online (All Devices)**  
 Online Offline Awaiting Contact  


**All Devices / Planned Changes, past 7 Days**  
 Planned Unplanned  


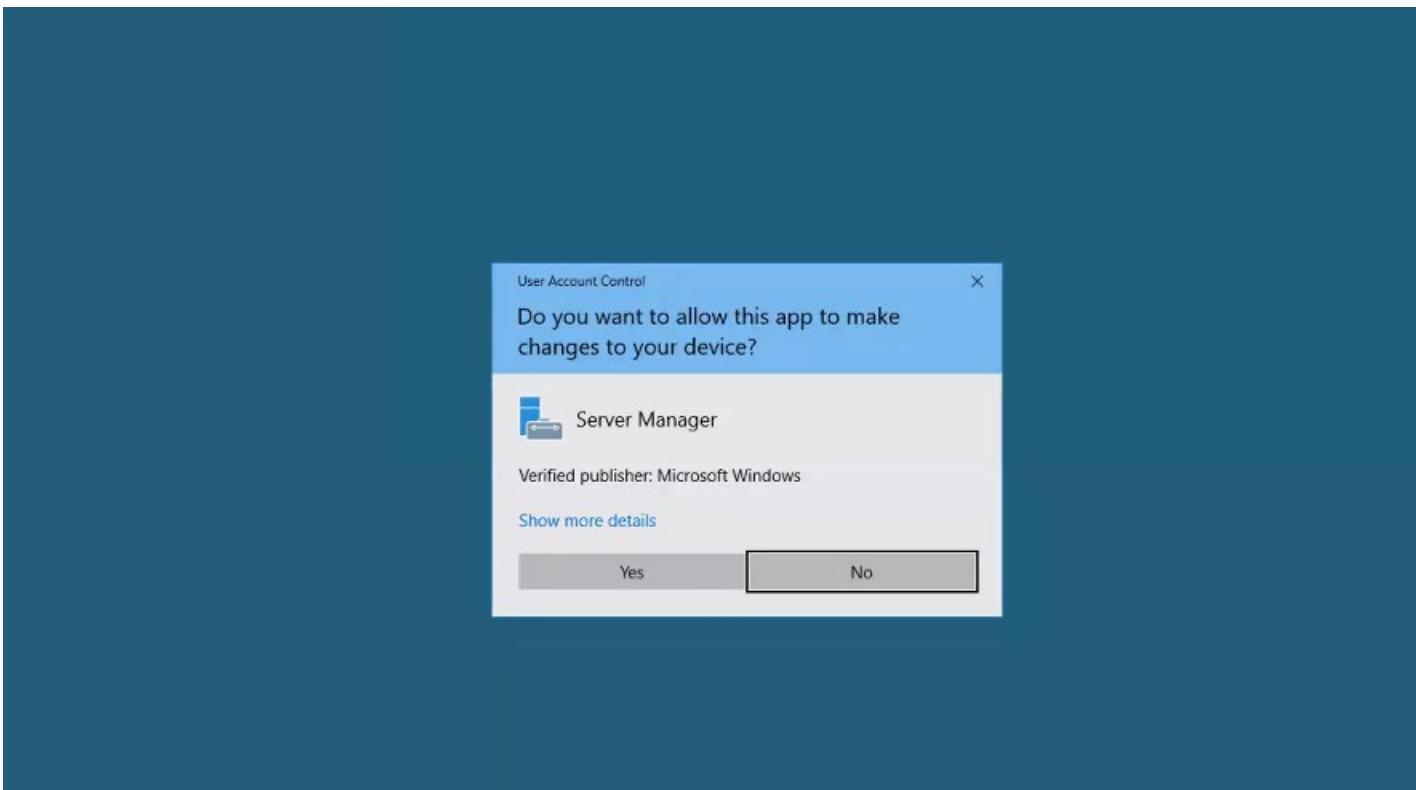
**Most Active Devices**  
 CIS-WRK-SHP-4 Total 24h Events: 662  


**Event Stream (Windows)**  
 Device Change Alert Error Audit  


**All Devices / Planned Changes, past 7 Days**  
 Planned Unplanned  


Welcome to Change Tracker

Getting Started Configure Tracking Template



## Run reports

Name	Total Recent Events	Last Poll Time	Groups	Templates	Agent Version
CIS-WRK-SHP-3	0	22 Nov 2019 20:29:14	Deleted		7.0.0.36
CIS-WRK-SHP-1	0	24 Jun 2021 10:11:01	Windows		7.0.0.37
CIS-WRK-SHP-4	5	24 Jun 2021 10:11:01	Windows 2016, Windows 2016 Remediation	CIS Windows Server 2016 Base Template	7.0.0.36
CIS-WRK-SHP-2	43	24 Jun 2021 10:11:01	Windows 2016, Windows 2016 Remediation	CIS Windows Server 2016 Base Template	7.0.0.36

Report Version : 1.0.0  
Average Score : 0.0 %  
Run Time : 24 Jun 2021 10:56:50

Device Name	24 Jun 2021 10:56:50	24 Jun 2021 10:56:54	24 Jun 2021 11:13:39
CIS-WRK-SHP-2	97.8 %	97.8 %	-
CIS-WRK-SHP-4	33.0 %	33.0 %	-

Select Report

- Windows 2016 / NNT CIS Microsoft Windows Server 2016 Benchmark...
- Windows 2016 / NNT CIS Microsoft Windows Server 2016 Benchmark - Level 1 Member Server**
- Windows 2016 Remediation / NNT Remediated CIS Microsoft Windows Server 2016 Benchmark - Level 1 Member Server

Recording

C:\User\WebinarUser\Desktop\NNT Remediated CIS Microsoft Windows Server 2016 Benchmark - Level 1 Member Server.xml NNT CIS Red Hat Enterprise Linux / Server Benchmark - Level 1.sh

```
<?xml version="1.0" encoding="UTF-8"?>
<StaticValue Value="1" />
</InputVariable>
<RuleExpression Rule="(eval:org.cisecurity.benchmarks.microsoft_windows_server_2016:obj:10239) == (eval:org.cisecurity.benchmarks.microsoft_windows_server_2016:ste:10132)" FailuresExpression="FAILED: (L1) Ensure 'Use
```

OperatingSystems>

</OperatingSystems>

</RuleExpression>

</Rule>

</SubCategory>

<Category>

</Section>

<Section Name="Windows Firewall With Advanced Security">

<Category Name="Domain Profile">

<SubCategory Name="Windows Firewall With Advanced Security Rules">

<Rule Number="9.1.1" Name="Remediated - (L1) Ensure 'Windows Firewall: Domain: Firewall state' is set to 'On (recommended)'>

<Description>Description: Select On (recommended) to have Windows Firewall with Advanced Security use the settings for this profile to filter network traffic. If you select Off, Windows Firewall with Advanced Security

<RuleExpression Rule="l=1" ShowFailuresExpression="Never" FailuresExpression="" ShowPassesExpression="WhenRulePasses" PassesExpression="Note: this test is not automatically evaluated. The rule has been deemed not suit

<OperatingSystems>

<OperatingSystemAll>/OperatingSystem

</OperatingSystems>

</RuleExpression>

<ResultText GeneralPreamble="Note: this test is not automatically evaluated. The rule has been deemed not suitable for the environment." ShowGeneralPreamble="Always" />

</Rule>

<Rule Number="9.1.2" Name="Remediated - (L1) Ensure 'Windows Firewall: Domain: Inbound connections' is set to 'Block (default)'>

<Description>Description: This setting determines the behavior for inbound connections that do not match an inbound firewall rule. The recommended state for this setting is: Block (default). Rationale: If the firewall a

<RuleExpression Rule="l=1" ShowFailuresExpression="Never" FailuresExpression="" ShowPassesExpression="WhenRulePasses" PassesExpression="Note: this test is not automatically evaluated. The rule has been deemed not suit

<OperatingSystems>

<OperatingSystemAll>/OperatingSystem

</OperatingSystems>

</RuleExpression>

<ResultText GeneralPreamble="Note: this test is not automatically evaluated. The rule has been deemed not suitable for the environment." ShowGeneralPreamble="Always" />

</Rule>

<Rule Number="9.1.3" Name="Remediated - (L1) Ensure 'Windows Firewall: Domain: Outbound connections' is set to 'Allow (default)'>

<Description>Description: This setting determines the behavior for outbound connections that do not match an outbound firewall rule. The recommended state for this setting is: Allow (default). Rationale: Some people bel

<RuleExpression Rule="l=1" ShowFailuresExpression="Never" FailuresExpression="" ShowPassesExpression="WhenRulePasses" PassesExpression="Note: this test is not automatically evaluated. The rule has been deemed not suit

<OperatingSystems>

<OperatingSystemAll>/OperatingSystem

</OperatingSystems>

</RuleExpression>

<ResultText GeneralPreamble="Note: this test is not automatically evaluated. The rule has been deemed not suitable for the environment." ShowGeneralPreamble="Always" />

</Rule>

<Rule Number="9.1.4" Name="Remediated - (L1) Ensure 'Windows Firewall: Domain: Settings: Display a notification' is set to 'No' (CCE Reference : CCE-38041-0)>

<Description>Description: Select this option to have Windows Firewall with Advanced Security display notifications to the user when a program is blocked from receiving inbound connections. The recommended state for this

<RuleExpression Rule="l=1" ShowFailuresExpression="Never" FailuresExpression="" ShowPassesExpression="WhenRulePasses" PassesExpression="Note: this test is not automatically evaluated. The rule has been deemed not suit

<OperatingSystems>

<OperatingSystemAll>/OperatingSystem

</OperatingSystems>

</RuleExpression>

<ResultText GeneralPreamble="Note: this test is not automatically evaluated. The rule has been deemed not suitable for the environment." ShowGeneralPreamble="Always" />

</Rule>

<Rule Number="9.1.5" Name="Remediated - (L1) Ensure 'Windows Firewall: Domain: Settings: Apply local firewall rules' is set to 'Yes (default)'>

<Description>Description: This setting controls whether local administrators are allowed to create local firewall rules that apply together with firewall rules configured by Group Policy. The recommended state for this

<RuleExpression Rule="l=1" ShowFailuresExpression="Never" FailuresExpression="" ShowPassesExpression="WhenRulePasses" PassesExpression="Note: this test is not automatically evaluated. The rule has been deemed not suit

<

xensible Markup Language file length:812,022 lines:4,856 ln:2,112 col:15 sel:0|0 Unix (LF) UTF-8 INS

NNT ChangeTracker Generation | CIS\_Microsoft\_Windows\_Server\_... | CIS-Contro... 199.188.127.130 Not secure | 10.5.66.37/#/devices

**Devices**

Active Query/Report: None GroupDevice: No Selections Online Status: All

Name	Total Recent Events	Last Poll Time	Groups	Templates	Agent Version
CIS-WRK-SHP-3	0	22 Nov 2019 20:29:14	Deleted		7.0.0.36
CIS-WRK-SHP-1	0	24 Jun 2021 10:11:01	Windows		7.0.0.37

Device Details Tracking Configuration Reports Event Stream

Device Name: CIS-WRK-SHP-1  
 Device Type: Windows (Master Proxy)  
 Last seen: 24 Jun 2021 10:14:01  
 Operating System: Windows Server 2016 Standard Evaluation  
 Member of Groups: All Devices, Windows  
 Compliance Reports: None  
 Tracking Templates: CHG345321, Manually Acknowledged Changes, NNT FAST Cloud White-listing Service 'validated safe changes'  
 Planned Changes: IP Address: 10.5.66.37  
 Associated Credentials: None  
 Agent Version: 7.0.0.37

CIS-WRK-SHP-4 5 24 Jun 2021 10:11:01 Windows 2016, Windows 2016 Remediation CIS Windows Server 2016 Base Template 7.0.0.36

Device Details Tracking Configuration Reports Event Stream

Device Name: CIS-WRK-SHP-4  
 Device Type: Windows (Master Proxy)  
 Last seen: 24 Jun 2021 10:11:01  
 Operating System: Windows Server 2016 Standard Evaluation  
 Member of Groups: All Devices, Windows, Windows 2016, Windows 2016 Remediation  
 Compliance Reports: None  
 Tracking Templates: CIS Windows Server 2016 Base Template (from Windows 2016)  
 Planned Changes: CHG345321, Manually Acknowledged Changes, NNT FAST Cloud White-listing Service 'validated safe changes', System Hardening Changes Detected  
 IP Address: 10.5.66.32  
 Associated Credentials: None  
 Agent Version: 7.0.0.36

CIS-WRK-SHP-2 43 24 Jun 2021 10:11:01 Windows 2016, Windows 2016 Remediation CIS Windows Server 2016 Base Template 7.0.0.36

1 - 4 of 4 items

<https://10.5.66.37/#/>

Recording 199.188.127.130 Not secure | 10.5.66.37/#/reports

**Reports and Queries**

Recent Group & Device Selections: No Selection Search

Search Groups: Search Devices: Date & Time Range: Past Hour Start Date: 06/24/2021 09:20:43 AM End Date: 06/24/2021 10:20:43 AM Show Advanced Options

Reports Filters: Report Type: Showing all Report Types Select Report Name-Contains Search Include Default System Reports Include All Users Reports

GroupDevice: No Selection Reports Output

Report or Query Name: Windows 2016 / NNT CIS Microsoft Windows Server 2016 Benchmark - Level 1 Member Server

Previous runs of this report are shown below. Preview or download them using layout template: Compliance Detail

Date	Description	Results available until	Actions
24 Jun 10:13:39	Windows 2016 / NNT CIS Microsoft Windows Server 2016 Benchmark - Level 1 Member Server: 1 of 2 reports complete	25 Jun 09:56:54	Preview Options Download Delete
24 Jun 09:56:54	Windows 2016 / NNT CIS Microsoft Windows Server 2016 Benchmark - Level 1 Member Server: 2 reports	25 Jun 09:56:54	Preview Options Download Delete
24 Jun 09:56:50	Windows 2016 / NNT CIS Microsoft Windows Server 2016 Benchmark - Level 1 Member Server: 2 reports	25 Jun 09:56:50	Preview Options Download Delete
23 Jun 22:34:18	Windows 2016 / NNT CIS Microsoft Windows Server 2016 Benchmark - Level 1 Member Server: 2 reports	Results available until 24 Jun 22:34:18	Preview Options Download Delete
	Windows 2016 Remediation / NNT Remediated CIS Microsoft Windows Server 2016 Benchmark - Level 1 Member Server		Preview Options Download Delete

1 - 4 of 4 items

\*C:\ProgramData\NNT\gen7agent.service\HubDetails.xml - Notepad++

File Edit Search View Encoding Language Settings Tools Macro Run Window ?

Remediation Script.bat HubDetails.xml

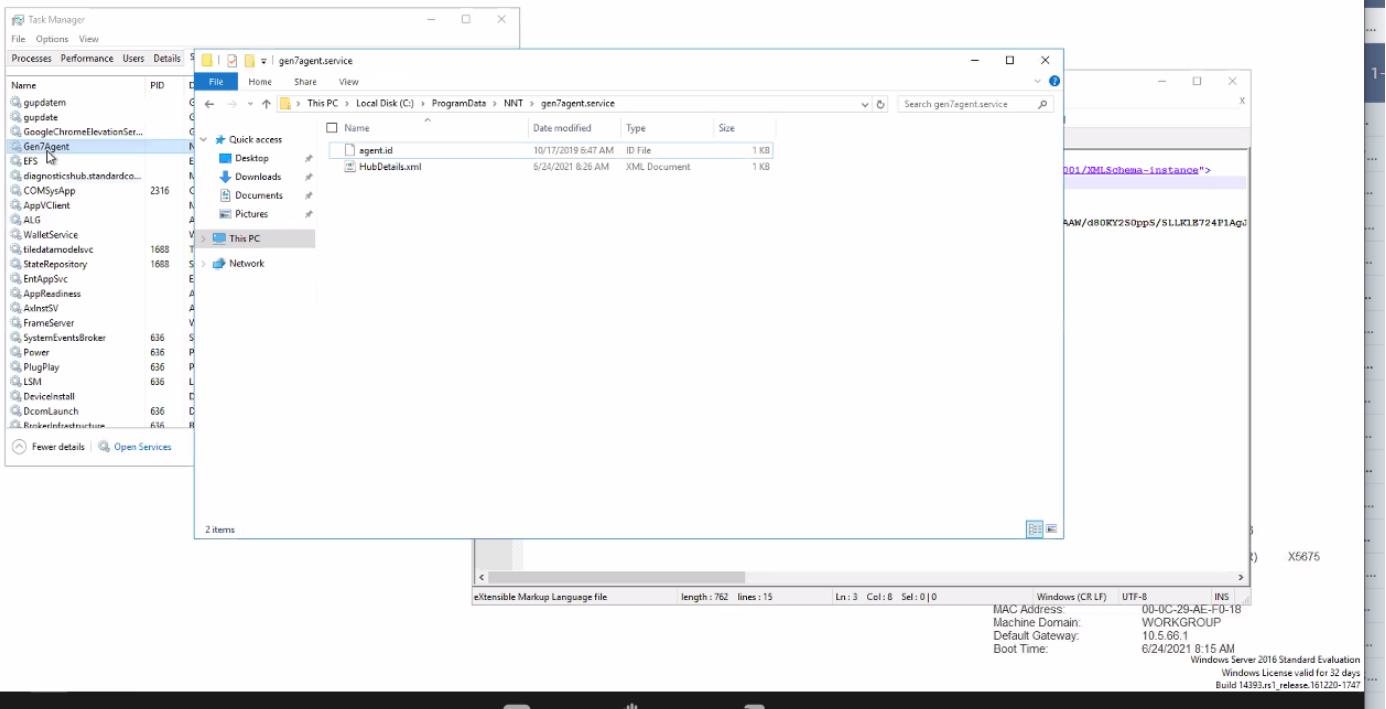
```

1 <?xml version="1.0" encoding="utf-8"?>
2 <HubDetails xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
3   <Url>https://10.5.66.37/api</Url>
4   <Username>agent</Username>
5   <Password />
6   <F1>AQAAANCMnd8BFdERjHoAwE/C1+sBAAAA1Pyea+TE8kaunsBA0YaKwAAAAACAAAAAAQZgAAAAAACAACAAAAAW/d80KY250ppS/SLLR1E724P1AgJ
7   <Proxy />
8   <ProxyDomain />
9   <ProxyUsername />
10  <ProxyPassword />
11  <UseDefaultProxy>false</UseDefaultProxy>
12  <NamePrefix />
13  <NameSuffix />
14  <Thumbprint />
15 </HubDetails>

```

eXtensible Markup Language file length : 762 lines : 15 Ln : 3 Col : 8 Sel : 0 | 0 Windows (CR LF) UTF-B INS .xml

CIS-WRK-SHP-4 199.188.127.130



Recording

Not secure | 10.5.66.37/#reports

NNT Dashboard Events Devices Compliance Reports Settings AmericaNew\_York Admin 199.188.127.130 10:28:22 7.2.1.21 (5878)

Groups & Devices Reports and Queries

Date & Time Range

Start Date: 06/24/2021 09:28:02 AM End Date: 06/24/2021 10:28:02 AM Show Advanced Options

Reports Filters Report Type Select Report Name-Contains Search

Include Default System Reports Include All Users Reports

Report or Query Name

24 Jun 10:23:44 Windows 2016 / NNT CIS Microsoft Windows Server 2016 Benchmark - Level 1 Member Server: 1 of 2 report complete

24 Jun 10:13:39 Windows 2016 / NNT CIS Microsoft Windows Server 2016 Benchmark - Level 1 Member Server: 1 of 2 report complete (1 with error / timeout) Results available until 25 Jun 10:13:39

24 Jun 09:56:54 Windows 2016 / NNT CIS Microsoft Windows Server 2016 Benchmark - Level 1 Member Server: 2 reports Results available until 25 Jun 09:56:54

24 Jun 09:56:50 Windows 2016 / NNT CIS Microsoft Windows Server 2016 Benchmark - Level 1 Member Server: 2 reports Results available until 25 Jun 09:56:50

23 Jun 22:34:18 Windows 2016 / NNT CIS Microsoft Windows Server 2016 Benchmark - Level 1 Member Server: 2 reports Results available until 24 Jun 22:34:18

Windows 2016 Remediation / NNT Remediated CIS Microsoft Windows Server 2016 Benchmark - Level 1 Member Server

24 Jun 10:23:46 Windows 2016 Remediation / NNT Remediated CIS Microsoft Windows Server 2016 Benchmark - Level 1 Member Server: 1 of 2 report complete

24 Jun 10:13:40 Windows 2016 Remediation / NNT Remediated CIS Microsoft Windows Server 2016 Benchmark - Level 1 Member Server: 1 of 2 report complete (1 with error / timeout) Results available until 25 Jun 10:13:40

24 Jun 09:56:55 Windows 2016 Remediation / NNT Remediated CIS Microsoft Windows Server 2016 Benchmark - Level 1 Member Server: 2 reports Results available until 25 Jun 09:56:55

24 Jun 09:56:53 Windows 2016 Remediation / NNT Remediated CIS Microsoft Windows Server 2016 Benchmark - Level 1 Member Server: 2 reports Results available until 25 Jun 09:56:53

23 Jun 22:34:17 Windows 2016 Remediation / NNT Remediated CIS Microsoft Windows Server 2016 Benchmark - Level 1 Member Server: 2 reports Results available until 24 Jun 22:34:17

1 - 5 of 5 items 21 - 22 of 22 items