

# STIG Implementation Report

- **Intern Credit Application For:** Bruce Thornton  
**Date:** 09/29/2025  
**STIG Finding:** WN11-CC-000204
  - **SRG:** [SRG-OS-000480-GPOS-00227](#)  
**Severity:** medium  
**Vulnerability ID:** V-253392 **CCI:** CCI-000366
- 

## 1. Introduction

This report documents the process of identifying, remediating, and verifying the fix for a Windows 11 STIG compliance finding. The selected finding was: STIG ID: WN11-CC-000204 "Enhanced diagnostic data must be limited to the minimum required to support Windows Analytics."

---

## 2. Initial Scan Results

- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)
- Finding ID: WN11-CC-000204
- Status: **Warning** (non-compliant)

 **Evidence:** First identified the STIG:

<https://stigaview.com/products/win11/v2r2/WN11-CC-000204/>

Initial scan result:

The screenshot shows the Tenable Vulnerability Management interface. The main header displays the scan name 'Win11DisaStigBruceSept29' and the status 'VULNERABILITY MANAGEMENT SCANS'. The left sidebar shows navigation options: 'Vulns by Plugin', 'Audits', 'Vulns by Asset', and 'History'. The main content area shows a search bar with 'WN11-CC-000204' and a results table. The table has columns for 'STATUS', 'NAME', 'FAMILY', and 'COUNT'. The first row shows a 'Warning' status for 'WN11-CC-000204 - Enhanced diagnostic data must be limited to t...' under the 'Windows Compliance Checks' family, with a count of 1. The right sidebar shows a summary of findings: 0 Critical Vulnerabilities, 0 High Vulnerabilities, 0 Medium Vulnerabilities, and 0 Low Vulnerabilities. Below this, the 'Scan Details' section shows: STATUS: Completed, START TIME: 09/29/2025 at 3:59 PM, TEMPLATE: Advanced Network Scan, SCANNER: LOCAL-SCAN-ENGINE-01, and TARGETS: 10.1.1.29.

\* The scan has returned a more urgent Status, however this status will be remediated to "Passed"

### 3. Manual Remediation Steps

Run "gpedit.msc"

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Data Collection and Preview Builds >> "Limit optional diagnostic data for Windows Analytics" to "Enabled" with "Enable Desktop Analytics collection" selected in "Options:"

Run "gpupdate /force" and restart.

Scan again,

- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)
- Finding ID: WN11-CC-000204
- Status: Passed

## Evidence:

The screenshot shows the Tenable Vulnerability Management interface. The top navigation bar includes the Tenable logo, 'Vulnerability Management', and a breadcrumb trail 'Scans > Scan Details'. On the right, there are 'Quick Actions' and user profile icons. The main header for the scan is 'Win11DisaStigBruceSept29' with a sub-header 'VULNERABILITY MANAGEMENT SCANS'. Below this, there are tabs for 'Vulns by Plugin', 'Audits' (selected), 'Vulns by Asset', and 'History'. A search bar contains 'WN11-CC-000204' and shows '1 Results'. A summary bar indicates '0 Failed', '0 Warning', and '1 Passed'. Below this is a table with 1 item. The table has columns for STATUS, NAME, FAMILY, and COUNT. The single row shows a 'Passed' status for the name 'WN11-CC-000204 - Enhanced diagnostic data must be limited to t...', with the family 'Windows Compliance Checks' and a count of '1'. On the right side, there are four vulnerability counts: '0 CRITICAL VULNERABILITIES', '0 HIGH VULNERABILITIES', '0 MEDIUM VULNERABILITIES', and '0 LOW VULNERABILITIES'. Below these is a 'Scan Details' section with fields for STATUS (Completed), START TIME (09/29/2025 at 4:29 PM), TEMPLATE (Advanced Network Scan), SCANNER (LOCAL-SCAN-ENGINE-01), and TARGETS (10.1.1.29).

STATUS	NAME	FAMILY	COUNT
Passed	WN11-CC-000204 - Enhanced diagnostic data must be limited to t...	Windows Compliance Checks	1

## 4. Reintroduction of Finding (Manually Undo Test)

To demonstrate full control of the setting, the fix was undone:

- Disabled the setting. Open Group Policy Management “gpedit.msc” and followed the instructions for remediation from before and set it to the original setting: “Not Configured.”
- Ran “`gpupdate /force`” and rescanned.

Status: Failed, Non-Compliant

## Evidence:

The screenshot shows the Tenable Vulnerability Management interface. The main header displays the scan name "Win11DisaStigBruceSept29" and the path "Scans > Scan Details". Below the header, there are tabs for "Vulns by Plugin", "Audits", "Vulns by Asset", and "History". The "Audits" tab is selected. A search bar contains the ID "WN11-CC-000204" and shows "1 Results". Below the search bar, there are three progress bars: "Failed" (1), "Warning" (1), and "Passed" (1). A table lists the scan results, showing one item with a "Failed" status. The table has columns for "STATUS", "NAME", "FAMILY", and "COUNT". The row shows "Failed", "WN11-CC-000204 - Enhanced diagnostic data must be limited to t...", "Windows Compliance Checks", and "1". On the right side, there is a "Scan Details" panel showing various metrics: "CRITICAL VULNERABILITIES" (0), "HIGH VULNERABILITIES" (0), "MEDIUM VULNERABILITIES" (0), and "LOW VULNERABILITIES" (0). It also shows the "STATUS" as "Completed", "START TIME" as "09/29/2025 at 4:57 PM", "TEMPLATE" as "Advanced Network Scan", "SCANNER" as "LOCAL-SCAN-ENGINE-01", and "TARGETS" as "10.1.1.29".

## 5. Remediation with PowerShell Script

Utilizing PowerShell ISE, this script was ran:

```
<#  
.SYNOPSIS  
Remediates STIG ID WN11-CC-000204:  
Limits enhanced diagnostic data to the minimum (Basic). Enhanced diagnostic data must be  
limited to the minimum required to support Windows Analytics.  
#>  
  
# Ensure running as Administrator  
If (-NOT ([Security.Principal.WindowsPrincipal]  
[Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole(  
[Security.Principal.WindowsBuiltinRole] "Administrator")) {  
    Write-Error "You must run this script as Administrator."  
    Exit 1  
}  
  
# Registry details  
$RegPath = "HKLM:\SOFTWARE\Policies\Microsoft\Windows\DataCollection"  
$RegName = "AllowTelemetry"
```

```
$RegValue = 1 # Basic
```

```
# Create path if missing
```

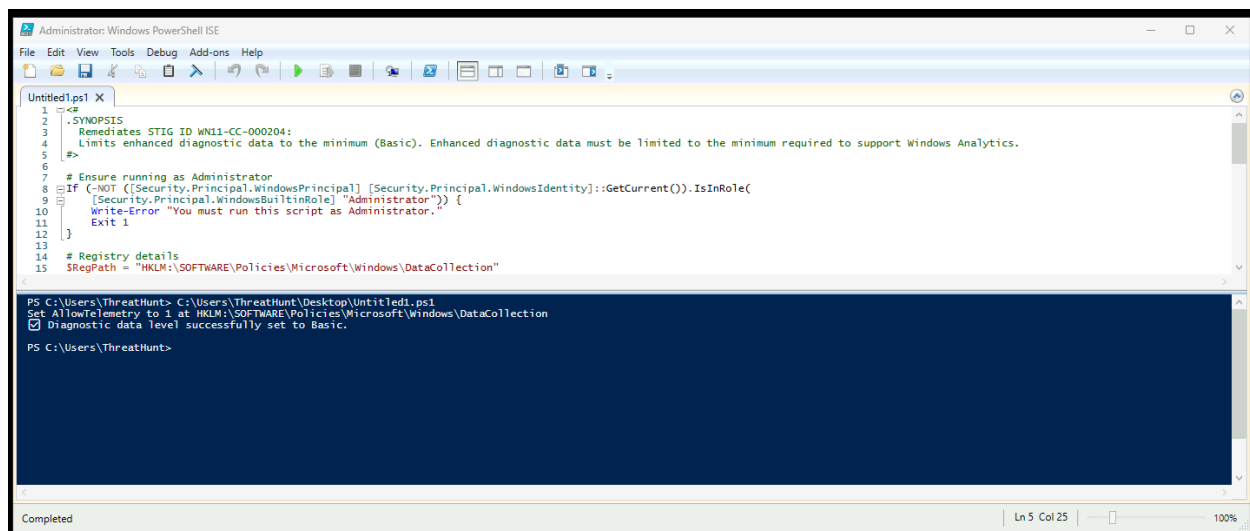
```
If (-Not (Test-Path $RegPath)) {  
    New-Item -Path $RegPath -Force | Out-Null  
    Write-Output "Created registry path: $RegPath"  
}
```

```
# Apply setting
```

```
Set-ItemProperty -Path $RegPath -Name $RegName -Value $RegValue -Type DWord  
Write-Output "Set $RegName to $RegValue at $RegPath"
```

```
# Verify
```

```
$CurrentValue = (Get-ItemProperty -Path $RegPath -Name $RegName).$RegName  
If ($CurrentValue -eq $RegValue) {  
    Write-Output "✅ Diagnostic data level successfully set to Basic."  
} Else {  
    Write-Error "❌ Failed to apply setting. Current value: $CurrentValue"  
}
```



The screenshot shows the Windows PowerShell ISE interface. The script file 'Untitled1.ps1' contains the following code:

```
1 #  
2 .SYNOPSIS  
3 Remediate STIG ID WN11-CC-000204:  
4 Limits enhanced diagnostic data to the minimum (Basic). Enhanced diagnostic data must be limited to the minimum required to support Windows Analytics.  
5  
6  
7 # Ensure running as Administrator  
8 If (-NOT ([Security.Principal.WindowsPrincipal] [Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole(  
9     [Security.Principal.WindowsBuiltInRole] "Administrator")) {  
10     Write-Error "You must run this script as Administrator."  
11     Exit 1  
12 }  
13  
14 # Registry details  
15 $RegPath = "HKLM:\SOFTWARE\Policies\Microsoft\Windows\DataCollection"
```

The console output shows the script execution results:

```
PS C:\Users\ThreatHunt> C:\Users\ThreatHunt\Desktop\Untitled1.ps1  
Set AllowTelemetry to 1 at HKLM:\SOFTWARE\Policies\Microsoft\Windows\DataCollection  
✅ Diagnostic data level successfully set to Basic.  
PS C:\Users\ThreatHunt>
```

The status bar at the bottom indicates 'Completed' and 'Ln 5 Col 25'.

Run "gpupdate /force" and restart.

Scan again,

- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)

- Finding ID: WN11-CC-000204
- Status: Passed

Evidence:

The screenshot displays the Tenable Vulnerability Management interface. At the top, the breadcrumb navigation shows 'Scans > Scan Details'. The main header identifies the scan as 'Win11DisaStigBruceSept29'. Below this, there are tabs for 'Vulns by Plugin', 'Audits', 'Vulns by Asset', and 'History'. A search bar contains the finding ID 'WN11-CC-000204', resulting in '1 Results'. A summary bar indicates '0 Failed', '0 Warning', and '1 Passed' results. A table lists the findings, showing one item with a 'Passed' status. The right sidebar provides 'Scan Details' including Status (Completed), Start Time (09/29/2025 at 5:22 PM), Template (Advanced Network Scan), Scanner (LOCAL-SCAN-ENGINE-01), and Targets (10.1.1.29).

## Notes

- Must run as **Administrator**.
- A **restart** or **gpupdate /force** may be required for Tenable to register the change.
- On **Windows 11 Home**, this policy may not exist or behave differently (but STIGs apply to Enterprise/Education builds).

## 6. Conclusion

The finding **WN11-CC-000204** was successfully:

- Detected in an initial Tenable STIG Audit scan,
- Remediated manually,
- Verified through a second scan,

- Undone and confirmed as vulnerable again,
- Finally re-applied through PowerShell automation, and validated with a third scan.

This demonstrates the ability to manage Windows STIG compliance both manually and through PowerShell automation.