

# STIG Implementation Report

- **Intern Credit Application For:** Bruce Thornton  
**Date:** 10/27/2025  
**STIG Finding:** WN11-CC-000120
  - **SRG:** [SRG-OS-000095-GPOS-00049](#)  
**Severity:** medium  
**Vulnerability ID:** V-253378 **CCI:** CCI-000381
- 

## 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-000120  
“The network selection user interface (UI) must not be displayed on the logon screen.”

---

## 2. Initial Scan Results

- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)
- Finding ID: WN11-CC-000120
- Status: **Failed** (non-compliant)

 **Evidence:** First identified the STIG:

<https://stigaview.com/products/win11/v2r3/WN11-CC-000120/>

Initial scan result:

The screenshot displays 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 icons for 'Quick Actions', help, notifications, settings, and a user profile 'BR'. The main header shows the scan name 'Windows11DisaStigScanBruce' and buttons for 'Export', 'Edit', and 'Trash'. Below the header, there are tabs for 'Vulns by Plugin', 'Audits', 'Vulns by Asset', and 'History'. A search bar contains 'WN11-CC-000120' and shows '1 Results'. A progress bar indicates 1 Failed, 0 Warning, and 0 Passed. A table lists the scan results:

STATUS	NAME	FAMILY	COUNT
Failed	WN11-CC-000120 - The network selection user interface (UI) mu...	Windows Compliance Checks	1

On the right side, a 'Scan Details' panel shows: STATUS: Completed, START TIME: 10/27/2025 at 8:52 PM, TEMPLATE: Advanced Network Scan, SCANNER: LOCAL-SCAN-ENGINE-01, and TARGETS: 10.1.0.149. At the top right of this panel, there are four vulnerability counts: 0 CRITICAL, 0 HIGH, 0 MEDIUM, and 0 LOW.

### 3. Manual Remediation Steps

Run "gpedit.msc"

Configure the policy value for Computer Configuration >> Administrative Templates >> System >> Logon >> "Do not display network selection UI" to "Enabled".

Run "gpupdate /force" and restart.

Scan again,

- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)
- Finding ID: WN11-CC-000120
- Status: **Passed**

Evidence:

The screenshot shows the Tenable Vulnerability Management interface. The main header displays 'tenable Vulnerability Management' and 'Scans > Scan Details'. The scan title is 'Windows11DisaStigScanBruce'. Below the title, there are tabs for 'Vulns by Plugin', 'Audits', 'Vulns by Asset', and 'History'. A search bar contains 'WN11-CC-000120' with '1 Results' shown. A progress bar indicates 0 Failed, 0 Warning, and 1 Passed. Below this, a table lists 1 item with columns for STATUS, NAME, FAMILY, and COUNT. The item is 'Passed' with the name 'WN11-CC-000120 - The network selection user interface (UI) mu...' and family 'Windows Compliance Checks'. On the right, a 'Scan Details' panel shows: STATUS: Completed, START TIME: 10/27/2025 at 9:20 PM, TEMPLATE: Advanced Network Scan, SCANNER: LOCAL-SCAN-ENGINE-01, and TARGETS: 10.1.0.149. Summary statistics on the right show 0 Critical, 0 High, 0 Medium, and 0 Low vulnerabilities.

## 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 after remediation. The main header displays 'tenable Vulnerability Management' and 'Scans > Scan Details'. The scan title is 'Windows11DisaStigScanBruce'. Below the title, there are tabs for 'Vulns by Plugin', 'Audits', 'Vulns by Asset', and 'History'. A search bar contains 'WN11-CC-000120' with '1 Results' shown. A progress bar indicates 1 Failed, 0 Warning, and 0 Passed. Below this, a table lists 1 item with columns for STATUS, NAME, FAMILY, and COUNT. The item is 'Failed' with the name 'WN11-CC-000120 - The network selection user interface (UI) mu...' and family 'Windows Compliance Checks'. On the right, a 'Scan Details' panel shows: STATUS: Completed, START TIME: 10/27/2025 at 9:56 PM, TEMPLATE: Advanced Network Scan, SCANNER: LOCAL-SCAN-ENGINE-01, and TARGETS: 10.1.0.149. Summary statistics on the right show 0 Critical, 0 High, 0 Medium, and 0 Low vulnerabilities.

## 5. Remediation with PowerShell Script

Save as: Remediate-WN11-CC-000120.ps1 and run **as Administrator** utilizing PowerShell ISE:

```
<#
.SYNOPSIS
    Remediates STIG WN11-CC-000120:
    Hides the network selection UI on the Windows logon screen.

.NOTES
    Run as Administrator. Logoff/reboot may be needed for logon screen to reflect the change.
#>

# Require admin
if (-not ([Security.Principal.WindowsPrincipal] [Security.Principal.WindowsIdentity]::GetCurrent()
).IsInRole([Security.Principal.WindowsBuiltInRole] "Administrator")) {
    Write-Error "Run this script as Administrator."
    exit 1
}

$RegPath = "HKLM:\SOFTWARE\Policies\Microsoft\Windows\System"
$RegName = "DontDisplayNetworkSelectionUI"
$RegValue = 1

# Ensure path exists
if (-not (Test-Path $RegPath)) {
    New-Item -Path $RegPath -Force | Out-Null
    Write-Output "Created registry path: $RegPath"
}

# Apply setting
New-ItemProperty -Path $RegPath -Name $RegName -Value $RegValue -PropertyType DWord
-Force | Out-Null
Write-Output "Set $RegName to $RegValue at $RegPath"

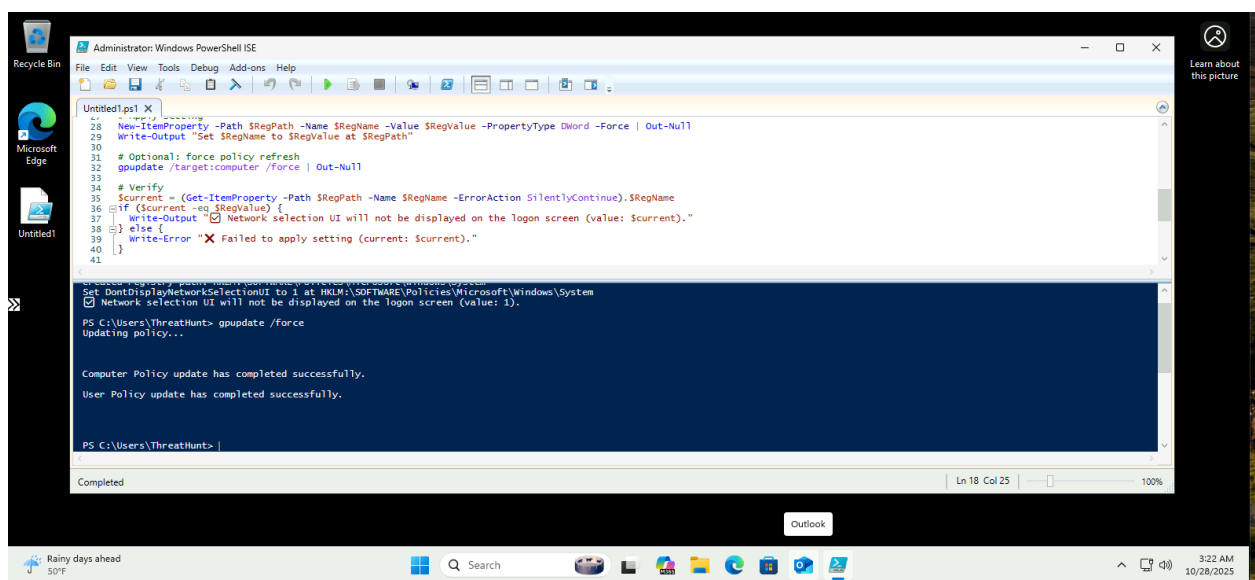
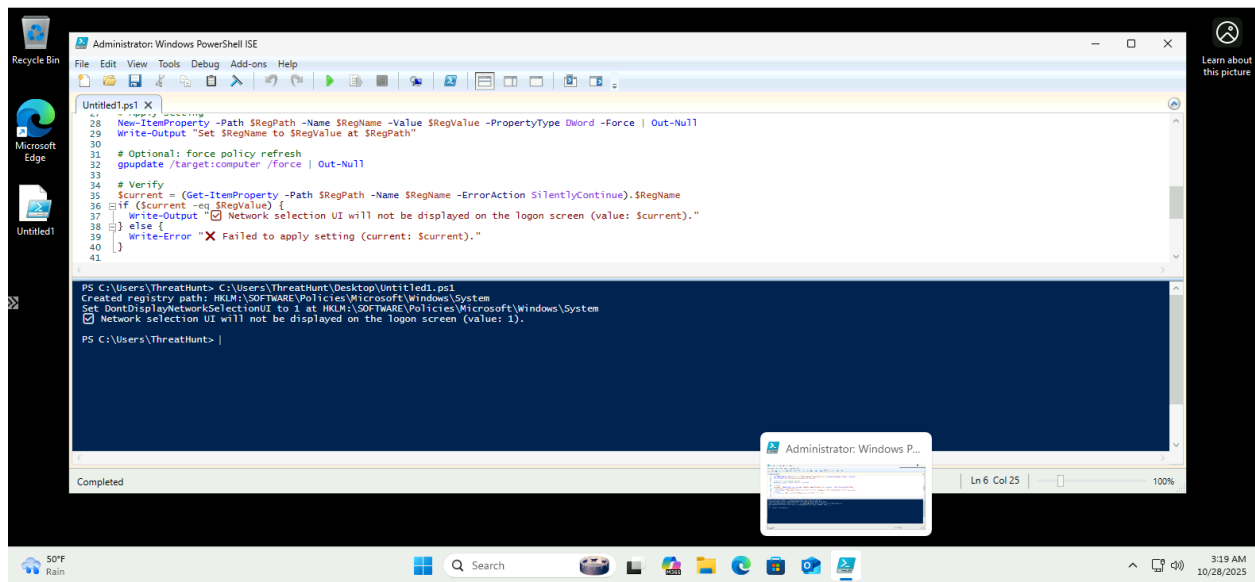
# Optional: force policy refresh
gpupdate /target:computer /force | Out-Null

# Verify
```

```

$current = (Get-ItemProperty -Path $RegPath -Name $RegName -ErrorAction
SilentlyContinue).$RegName
if ($current -eq $RegValue) {
    Write-Output "✅ Network selection UI will not be displayed on the logon screen (value:
$current)."
} else {
    Write-Error "❌ Failed to apply setting (current: $current)."
}

```



Run “gpupdate /force” and restart.

Scan again,

- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)
- Finding ID: WN11-CC-000120
- Status: **Passed**

Evidence:

The screenshot displays the Tenable Vulnerability Management interface. The main header shows 'tenable Vulnerability Management' and 'Scans > Scan Details'. The scan title is 'Windows11DisaStigScanBruce'. Below the title, there are tabs for 'Vulns by Plugin', 'Audits', 'Vulns by Asset', and 'History'. The 'Audits' tab is selected, showing a search bar with 'WN11-CC-000120' and '1 Results'. A summary bar indicates '0 Failed', '0 Warning', and '1 Passed'. Below this, a table lists the audit results:

STATUS	NAME	FAMILY	COUNT
Passed	WN11-CC-000120 - The network selection user interface (UI) mu...	Windows Compliance Checks	1

On the right side, there are sections for 'Vulnerabilities' (0 Critical, 0 High, 0 Medium, 0 Low) and 'Scan Details' (Status: Completed, Start Time: 10/27/2025 at 10:25 PM, Template: Advanced Network Scan, Scanner: LOCAL-SCAN-ENGINE-01, Targets: 10.1.0.149).

## What it sets

- **GPO:** Computer Config → Admin Templates → System → Logon → **Do not display network selection UI**
- **Registry:** HKLM\SOFTWARE\Policies\Microsoft\Windows\System → DontDisplayNetworkSelectionUI (DWORD) = 1

## Notes

- Tenable/Nessus typically checks that **DontDisplayNetworkSelectionUI=1** under HKLM\SOFTWARE\Policies\Microsoft\Windows\System.

- Change takes effect at the **next logon**; a **reboot or logoff** helps ensure the lock/Welcome screen reflects it.
  - This is **computer-scope** (HKLM), so you don't need per-user actions.
- 

## 6. Conclusion

The finding **WN11-CC-000120** 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.