

STIG Implementation Report

- **Intern Credit Application For:** Bruce Thornton
Date: 10/12/2025
STIG Finding: WN11-CC-000195
 - **SRG:** [SRG-OS-000480-GPOS-00227](#)
Severity: medium
Vulnerability ID: V-253389 **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-000195 “Enhanced anti-spoofing for facial recognition must be enabled on Windows 11.”

2. Initial Scan Results

- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)
- Finding ID: WN11-CC-000195
- Status: **Warning** (non-compliant)

 **Evidence:** First identified the STIG:

<https://stigaview.com/products/win11/v2r2/WN11-CC-000195/>

Initial scan result:

The screenshot displays the Tenable Vulnerability Management interface. At the top, the navigation bar includes the Tenable logo, 'Vulnerability Management', and a breadcrumb trail 'Scans > Scan Details'. A 'Quick Actions' dropdown menu is visible on the right. The main header shows the scan name 'Win11DisaStigBruceSept12' and a search bar containing 'WN11-CC-000195'. Below the header, there are tabs for 'Vulns by Plugin', 'Audits', 'Vulns by Asset', and 'History'. The 'Audits' tab is active, showing a summary of results: 1 Failed, 1 Warning, and 1 Passed. A table below this summary lists the audit details. The table has columns for 'STATUS', 'NAME', 'FAMILY', and 'COUNT'. One item is listed with a status of 'Failed', name 'WN11-CC-000195 - Enhanced anti-spoofing for facial recognition ...', family 'Windows Compliance Checks', and count '1'. On the right side of the interface, there is a 'Scan Details' panel. It shows a summary of vulnerabilities: 0 Critical, 0 High, 0 Medium, and 0 Low. Below this, it lists the scan status as 'Completed', the start time as '10/12/2025 at 3:11 PM', the template as 'Advanced Network Scan', and the scanner as 'LOCAL-SCAN-ENGINE-01'. The targets are listed as '10.1.0.136'.

STATUS	NAME	FAMILY	COUNT
Failed	WN11-CC-000195 - Enhanced anti-spoofing for facial recognition ...	Windows Compliance Checks	1

3. Manual Remediation Steps

Run "gpedit.msc"

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Biometrics >> Facial Features >> "Configure enhanced anti-spoofing" to "Enabled".

Run "gpupdate /force" and restart.

Scan again,

- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)
- Finding ID: WN11-CC-000195sudo
- 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'. A 'Quick Actions' dropdown is visible. The main header displays the scan name 'Win11DisaStigBruceSept12' and buttons for 'Export', 'Edit', and 'Trash'. Below the header, 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-000195' and '1 Results'. A progress bar indicates 0 Failed, 0 Warning, and 1 Passed. Below this, a table lists 1 item with the following details:

STATUS	NAME	FAMILY	COUNT
Passed	WN11-CC-000195 - Enhanced anti-spoofing for facial recognition ...	Windows Compliance Checks	1

On the right side, a 'Scan Details' panel shows the following information:

- CRITICAL VULNERABILITIES: 0
- HIGH VULNERABILITIES: 0
- MEDIUM VULNERABILITIES: 0
- LOW VULNERABILITIES: 0
- STATUS: Completed
- START TIME: 10/12/2025 at 3:46 PM
- TEMPLATE: Advanced Network Scan
- SCANNER: LOCAL-SCAN-ENGINE-01
- TARGETS: 10.1.0.136

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 top navigation bar includes the Tenable logo, 'Vulnerability Management', and a breadcrumb trail 'Scans > Scan Details'. A 'Quick Actions' dropdown is visible. The main header displays the scan name 'Win11DisaStigBruceSept12' and buttons for 'Export', 'Edit', and 'Trash'. Below the header, 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-000195' and '1 Results'. A progress bar indicates 1 Failed, 0 Warning, and 0 Passed. Below this, a table lists 1 item with the following details:

STATUS	NAME	FAMILY	COUNT
Failed	WN11-CC-000195 - Enhanced anti-spoofing for facial recognition ...	Windows Compliance Checks	1

On the right side, a 'Scan Details' panel shows the following information:

- CRITICAL VULNERABILITIES: 0
- HIGH VULNERABILITIES: 0
- MEDIUM VULNERABILITIES: 0
- LOW VULNERABILITIES: 0
- STATUS: Completed
- START TIME: 10/12/2025 at 4:23 PM
- TEMPLATE: Advanced Network Scan
- SCANNER: LOCAL-SCAN-ENGINE-01
- TARGETS: 10.1.0.136

5. Remediation with PowerShell Script

Utilizing PowerShell ISE this script was saved and ran:

```
<#
.SYNOPSIS
Remediates STIG WN11-CC-000195:
Enables enhanced anti-spoofing for Windows Hello Face.

.NOTES
Run as Administrator. A gpupdate/reboot may be required for scanners 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\Biometrics\FacialFeatures"
$RegName = "EnhancedAntiSpoofing"
$RegValue = 1

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

# Set value
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 "✅ Enhanced anti-spoofing policy is enabled."
} else {
    Write-Error "❌ Failed to enable enhanced anti-spoofing (current: $current)."
}

```

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 main header indicates the scan is for 'Win11DisaStigBruceSept12'. The 'Audits' tab is selected, showing a search for 'WN11-CC-000195' with 1 result. The results table shows 1 item with a status of 'Passed'. The right sidebar provides a summary of vulnerabilities (0 Critical, 0 High, 0 Medium, 0 Low) and scan details including the status 'Completed', start time '10/12/2025 at 4:39 PM', template 'Advanced Network Scan', scanner 'LOCAL-SCAN-ENGINE-01', and target '10.1.0.136'.

- **Note:** Passing compliance also depends on the device supporting Windows Hello Face with anti-spoofing (IR camera). If hardware doesn’t support it, scanners can still flag it even with the key set—in that case you’d document a waiver/POA&M.

6. Conclusion

The finding **WN11-CC-000195** 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.