

# STIG Implementation Report

- **Intern Credit Application For:** Bruce Thornton  
**Date:** 11/13/2025  
**STIG Finding:** WN11-CC-000005
  - **SRG:** [SRG-OS-000095-GPOS-00049](#)  
**Severity:** medium  
**Vulnerability ID:** V-253350 **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-000005 “Camera access from the lock screen must be disabled.”

---

## 2. Initial Scan Results

- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)
- Finding ID: WN11-CC-000005
- Status: **Failed** (non-compliant)



**Evidence:** First identified the STIG:

<https://stigaview.com/products/win11/v2r3/WN11-CC-000005/>

Initial scan result:

The screenshot shows the Tenable Vulnerability Management interface. At the top, it says "Scans > Scan Details > Audit Details". Below that, the title is "WN11-CC-000005 - Camera access from the lock screen must be disabled." A red "FAILED" button is visible. The main area shows a table with one result, where the status is "FAILED" and the name is "10.1.0.152". On the right side, there's a "Solution" section with instructions to configure policy values in Computer Configuration > Administrative Templates > Control Panel > Personalization. It also includes a "See Also" link to a STIG file and a "Reference Information" table comparing various policy settings across different categories like CAT, CN-L3, and CSF.

### 3. Manual Remediation Steps

Ran gpedit.msc:

If the device does not have a camera, this is NA.

Configure the policy value for Computer Configuration >> Administrative Templates >> Control Panel >> Personalization >> "Prevent enabling lock screen camera" to "Enabled".

Run “gpupdate /force” and restart.

Scan again,

- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)
- Finding ID: WN11-CC-000005
- Status: **Passed**

## Evidence:

The screenshot shows the Tenable Vulnerability Management interface. At the top, it says "Vulnerability Management" and "Scans > Scan Details". The scan name is "Win11Bruce1113DS". On the right, there are "Quick Actions" buttons and a "BR" button. Below the title, it says "VULNERABILITY MANAGEMENT SCANS". There are tabs for "Vuuls by Plugin", "Audits" (which is selected), "Vuuls by Asset", and "History". A search bar shows "WN11-CC-000005". The main area displays "1 Results". A progress bar at the top indicates 0 Failed, 0 Warning, 1 Passed, and 0 Critical. Below this, a table shows 1 item: "WN11-CC-000005 - Camera access from the lock screen must be..." under the "NAME" column, with "Windows Compliance Checks" under "FAMILY" and a count of 1. To the right, "Scan Details" are listed: STATUS (Completed), START TIME (11/13/2025 at 12:13 PM), TEMPLATE (Advanced Network Scan), SCANNER (LOCAL-SCAN-ENGINE-01), and TARGETS (10.1.0.152). On the far right, there are sections for CRITICAL VULNERABILITIES (0), HIGH VULNERABILITIES (0), MEDIUM VULNERABILITIES (0), and LOW VULNERABILITIES (0).

## 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.
- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)
- Finding ID: WN11-CC-000005

Status: **Failed**, Non-Compliant

## Evidence:

The screenshot shows the Tenable Vulnerability Management interface. At the top, it says "Vulnerability Management" and "Scans > Scan Details". The main area is titled "Win11Bruce1113DS" and "VULNERABILITY MANAGEMENT SCANS". Below this, there are tabs for "Vuuls by Plugin", "Audits" (which is selected), "Vuuls by Asset", and "History". A search bar at the top of the audit table shows "WN11-CC-000005" with "1 Results". The audit table has columns for "STATUS" (Failed, Warning, Passed), "NAME", "FAMILY", and "COUNT". One row is shown: "Failed" for "WN11-CC-000005 - Camera access from the lock screen must be..." under "Windows Compliance Checks". To the right of the table, "Scan Details" are listed: STATUS Completed, START TIME 11/13/2025 at 12:26 PM, TEMPLATE Advanced Network Scan, SCANNER LOCAL-SCAN-ENGINE-01, and TARGETS 10.1.0.152. On the far right, there are sections for CRITICAL VULNERABILITIES (0), HIGH VULNERABILITIES (0), MEDIUM VULNERABILITIES (0), and LOW VULNERABILITIES (0).

## 5. Remediation with PowerShell Script

Save as: Remediate-WN11-CC-000005.ps1 and run **as Administrator** utilizing PowerShell ISE:

The screenshot shows the Windows PowerShell ISE window. The title bar says "Administrator: Windows PowerShell ISE". The code pane contains a script named "Remediate-WN11-CC-000005.ps1" with the following content:

```
1
2
3 <#
4 STIG ID : WN11-CC-000005
5 Title : Camera access from the lock screen must be disabled.
6 ComputerName : $ComputerName
7 RegistryPath : 'HKLM\Software\Policies\Microsoft\Windows\Personalization'
8 NoLockScreenCamera (REG_DWORD) = 1
9 >
10
11 $regPath      = 'HKLM:\Software\Policies\Microsoft\Windows\Personalization'
12 $valueName    = 'NoLockScreenCamera'
13 $desiredValue = 1
14 $stigid       = 'WN11-CC-000005'
```

The output pane shows the execution of the script:

```
PS C:\Users\ThreatHunt> C:\Users\ThreatHunt\Desktop\Remediate-WN11-CC-000005.ps1
```

ComputerName	: Win11MBruce
STIG_ID	: WN11-CC-000005
Severity	: High
RegistryPath	: HKLM\Software\Policies\Microsoft\Windows\Personalization
ValueName	: NoLockScreenCamera
Requirement	: 1
ActionValue	: 1
ComplianceStatus	: Compliant
ActionTaken	: Created NoLockScreenCamera and set to 1.
Timestamp	: 11/13/2025 6:39:51 PM

The status bar at the bottom indicates "Completed".

## Script Used:

```

<#
STIG ID : WN11-CC-000005
Title : Camera access from the lock screen must be disabled.
Check/Fix mapping:
    HKLM\SOFTWARE\Policies\Microsoft\Windows\Personalization
        NoLockScreenCamera (REG_DWORD) = 1
#>

$regPath      = 'HKLM:\SOFTWARE\Policies\Microsoft\Windows\Personalization'
$valueName    = 'NoLockScreenCamera'
$desiredValue = 1
$stigId       = 'WN11-CC-000005'

# Ensure key exists
if (-not (Test-Path $regPath)) { New-Item -Path $regPath -Force | Out-Null }

# Set value if needed
$current = Get-ItemProperty -Path $regPath -Name $valueName -ErrorAction SilentlyContinue
if ($null -eq $current) {
    New-ItemProperty -Path $regPath -Name $valueName -PropertyType DWord -Value
    $desiredValue -Force | Out-Null
    $action = "Created $valueName and set to $desiredValue."
} elseif ($current.$valueName -ne $desiredValue) {
    Set-ItemProperty -Path $regPath -Name $valueName -Value $desiredValue -Type DWord
    $action = "Updated $valueName from $($current.$valueName) to $desiredValue."
} else {
    $action = "$valueName already set to $desiredValue. No change needed."
}

# Verify
$actual = (Get-ItemProperty -Path $regPath -Name $valueName -ErrorAction
SilentlyContinue).$valueName
$compliant = if ($actual -eq $desiredValue) {'Compliant'} else {'Non-Compliant'}

# Evidence object
[pscustomobject]@{
    ComputerName   = $env:COMPUTERNAME
    STIG_ID        = $stigId
    SettingName    = 'Prevent enabling lock screen camera'
    RegistryPath   = 'HKLM\SOFTWARE\Policies\Microsoft\Windows\Personalization'
    ValueName      = $valueName
    RequiredValue  = $desiredValue
    ActualValue    = $actual
    ComplianceStatus = $compliant
}

```

```
ActionTaken      = $action
Timestamp       = Get-Date
} | Format-List *
```

## Evidence:

The screenshot shows the Tenable Vulnerability Management interface. The top navigation bar includes 'Quick Actions', a search icon, a bell icon, and a 'BR' button. Below the header, the scan name is 'Win11Bruce113DS'. The main content area displays a summary of vulnerabilities: 0 Failed, 0 Warning, and 1 Passed. A detailed table lists one item: 'WN11-CC-000005 - Camera access from the lock screen must be...', categorized under 'Windows Compliance Checks'. On the right side, 'Scan Details' provide information about the status (Completed), start time (11/13/2025 at 12:44 PM), template (Advanced Network Scan), scanner (LOCAL-SCAN-ENGINE-01), and targets (10.1.0.152). The interface also features tabs for 'Vulns by Plugin', 'Audits', 'Vulns by Asset', and 'History'.

## 6. Conclusion

The finding **WN11-CC-000005** 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.