STIG Implementation Report

- **Intern Credit Application For:** Bruce Thornton
  Date: 11/12/2025
  STIG Finding: WN11-CC-000170
- **SRG:** SRG-OS-000480-GPOS-00227
  Severity: medium
  Vulnerability ID: V-253384 **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-000170 “The setting to allow Microsoft accounts to be optional for modern style apps must be enabled.”

---

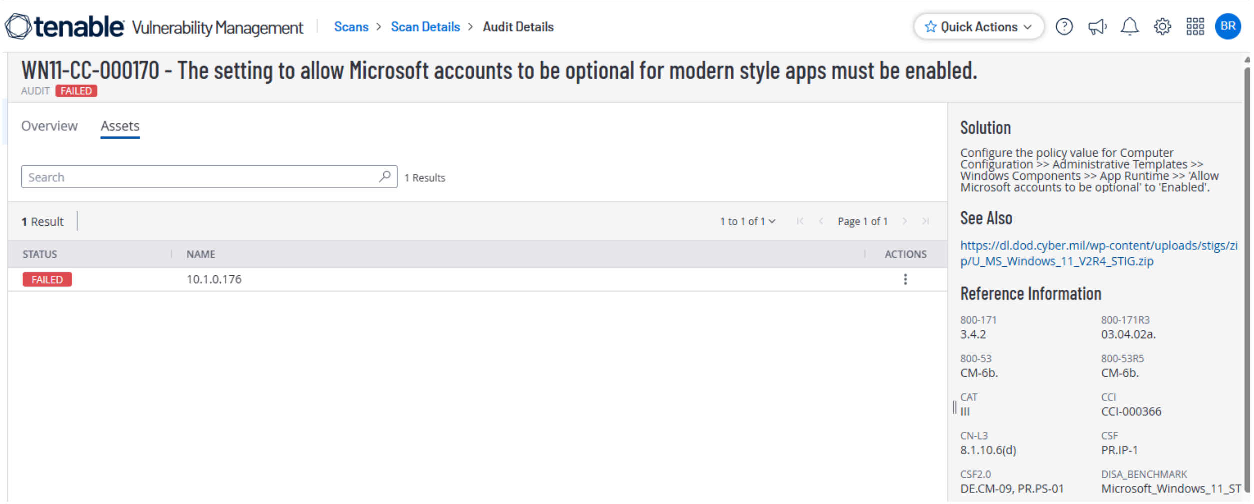
2. Initial Scan Results

- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)
- Finding ID: WN11-CC-000170
- Status: **Failed** (non-compliant)

📎 **Evidence:** First identified the STIG:

https://stigaview.com/products/win11/v2r2/WN11-CC-000170/

Initial scan result:


tenable Vulnerability Management
Scans > Scan Details > Audit Details
Quick Actions
BR
Overview
Assets
Search

WN11-CC-000170 - The setting to allow Microsoft accounts to be optional for modern style apps must be enabled.

AUDIT FAILED

1 Results

1 Result 1 to 1 of 1 Page 1 of 1

STATUS	NAME	ACTIONS
FAILED	10.1.0.176	⋮

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> App Runtime >> 'Allow Microsoft accounts to be optional' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

Reference Information

800-171 3.4.2	800-171R3 03.04.02a.
800-53 CM-6b.	800-53R5 CM-6b.
CAT III	CCI CCI-000366
CN-L3 8.1.10.6(d)	CSF PR.IP-1
CSF2.0 DE.CM-09, PR.PS-01	DISA_BENCHMARK Microsoft_Windows_11_ST

3. Manual Remediation Steps

Ran gpedit.msc:

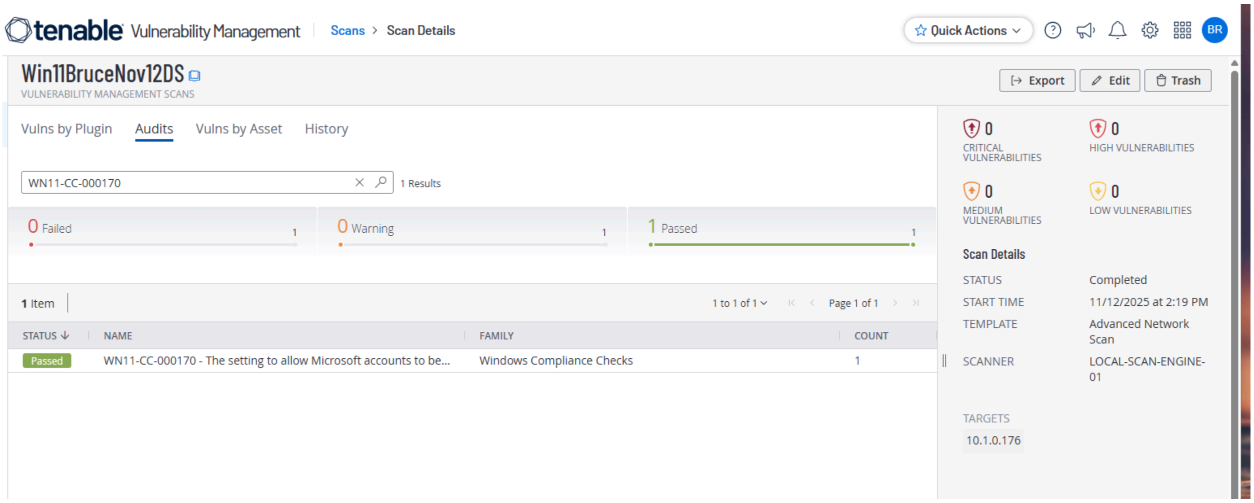
Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> App Runtime >> "Allow Microsoft accounts to be optional" to "Enabled".

Run “gpupdate /force” and restart.

Scan again,

- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)
- Finding ID: WN11-CC-000170
- Status: **Passed**

Evidence:



Win11BruceNov12DS

VULNERABILITY MANAGEMENT SCANS

WN11-CC-000170 — 1 Results

0 Failed 1 | 0 Warning 1 | 1 Passed 1

1 Item — 1 to 1 of 1 — Page 1 of 1

STATUS	NAME	FAMILY	COUNT
Passed	WN11-CC-000170 - The setting to allow Microsoft accounts to be...	Windows Compliance Checks	1

0 CRITICAL VULNERABILITIES — 0 HIGH VULNERABILITIES

0 MEDIUM VULNERABILITIES — 0 LOW VULNERABILITIES

Scan Details

STATUS	Completed
START TIME	11/12/2025 at 2:19 PM
TEMPLATE	Advanced Network Scan
SCANNER	LOCAL-SCAN-ENGINE-01

TARGETS

10.1.0.176

---

4. Reintroduction of Finding (Manually Undo Test)

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

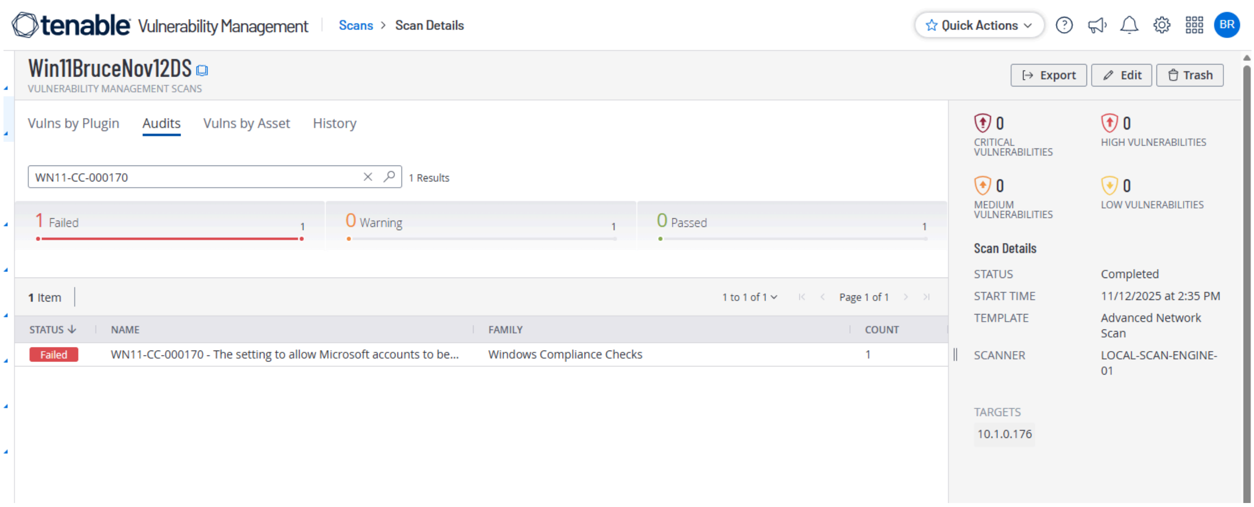
- Disabled the setting. Open Group Policy Management “gpedit.msc” and followed the instructions for remediation from before and set it to the original setting: “Not Configured”

- Ran “`gpupdate /force`” and rescanned.
- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)

- Finding ID: WN11-CC-000170

Status: **Failed**, Non-Compliant

Evidence:



Win11BruceNov12DS
VULNERABILITY MANAGEMENT SCANS

Search: WN11-CC-000170 — 1 Results

1 Failed 1 | 0 Warning 1 | 0 Passed 1

1 Item — 1 to 1 of 1 — Page 1 of 1

STATUS	NAME	FAMILY	COUNT
Failed	WN11-CC-000170 - The setting to allow Microsoft accounts to be...	Windows Compliance Checks	1

0 CRITICAL VULNERABILITIES
0 HIGH VULNERABILITIES
0 MEDIUM VULNERABILITIES
0 LOW VULNERABILITIES

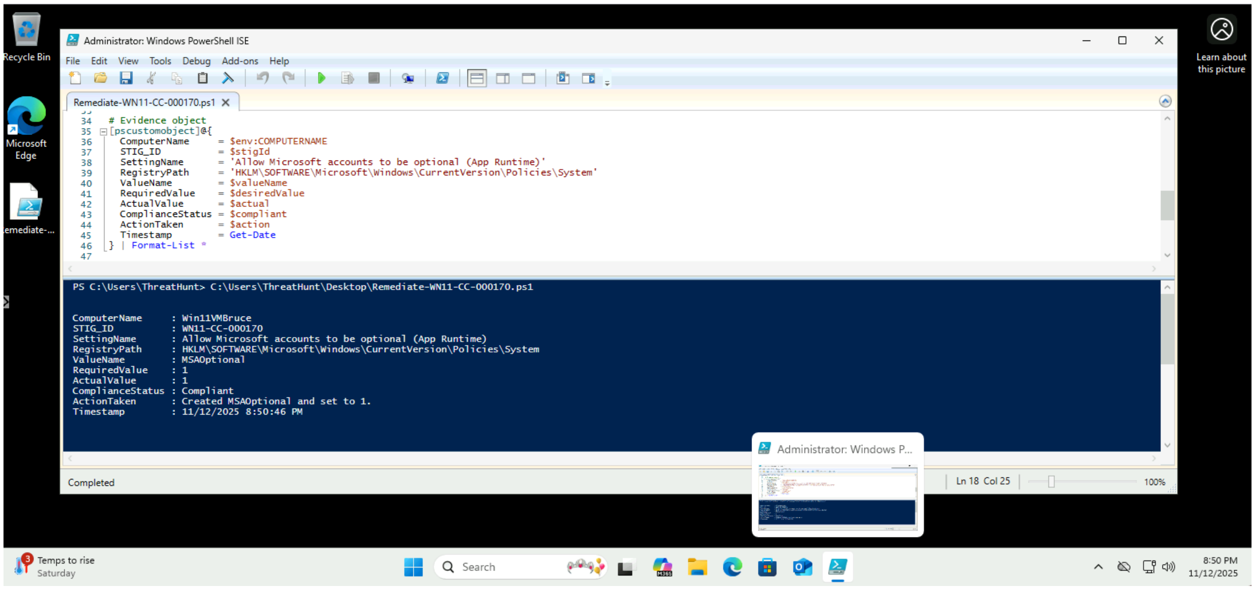
Scan Details

STATUS	Completed
START TIME	11/12/2025 at 2:35 PM
TEMPLATE	Advanced Network Scan
SCANNER	LOCAL-SCAN-ENGINE-01

TARGETS
10.1.0.176

5. Remediation with PowerShell Script

Save as: `Remediate-WN11-CC-000170.ps1` and run **as Administrator** utilizing PowerShell ISE:


Recycle Bin
Microsoft Edge
emediate-...
Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Remediate-WN11-CC-000170.ps1
Learn about this picture
Administrator: Windows P...
Ln 18 Col 25
100%
Temps to rise
Saturday
Search
8:50 PM
11/12/2025

```
# Evidence object
[pscustomobject]@{
  ComputerName      = $env:COMPUTERNAME
  STIG_ID           = $stigId
  SettingName       = 'Allow Microsoft accounts to be optional (App Runtime)'
  RegistryPath      = 'HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System'
  ValueName         = $valueName
  RequiredValue     = $desiredValue
  ActualValue       = $actual
  ComplianceStatus = $compliant
  ActionTaken       = $action
  Timestamp         = Get-Date
} | Format-List *
```

```
PS C:\Users\ThreatHunt> C:\Users\ThreatHunt\Desktop\Remediate-WN11-CC-000170.ps1


ComputerName     : Win11VMBruce
STIG_ID          : WN11-CC-000170
SettingName      : Allow Microsoft accounts to be optional (App Runtime)
RegistryPath     : HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
ValueName        : MSAOptional
RequiredValue    : 1
ActualValue      : 1
ComplianceStatus : Compliant
ActionTaken      : Created MSAOptional and set to 1.
Timestamp        : 11/12/2025 8:50:46 PM
```

Completed

Script Used:

```
<#
STIG ID : WN11-CC-000170
Title   : The setting to allow Microsoft accounts to be optional for modern style apps must be
enabled.

Check/Fix mapping:
  HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
  Value: MSAOptional (REG_DWORD) = 1  # Enabled
#>

$regPath      = 'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System'
$valueName    = 'MSAOptional'
$desiredValue = 1
$stigId       = 'WN11-CC-000170'

# 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      = 'Allow Microsoft accounts to be optional (App Runtime)'
  RegistryPath     = 'HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System'
  ValueName        = $valueName
  RequiredValue    = $desiredValue
```

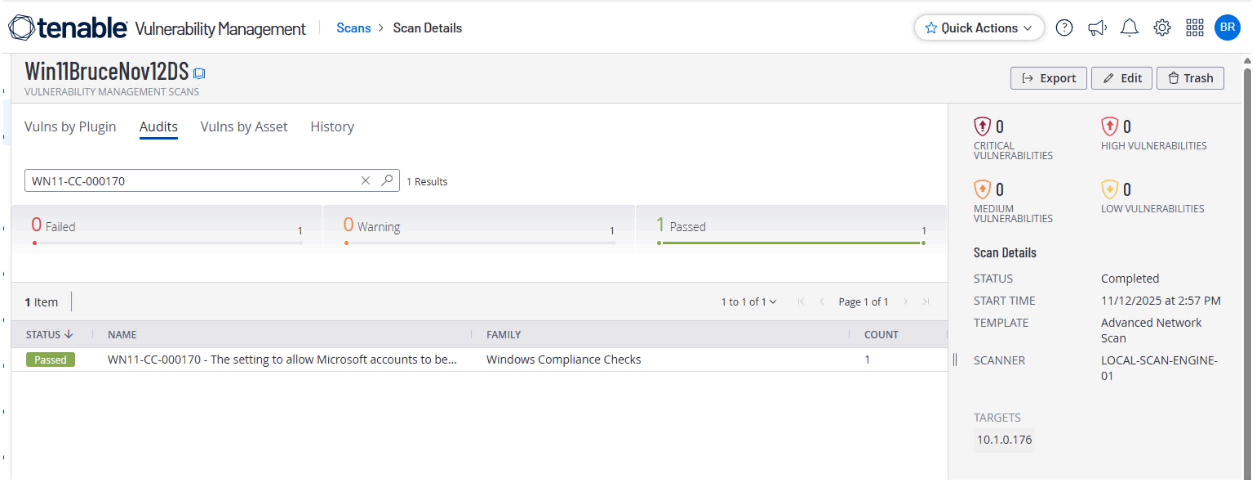
```
 ActualValue      = $actual
 ComplianceStatus = $compliant
 ActionTaken      = $action
 Timestamp        = Get-Date
} | Format-List *
```

Run “gpupdate /force” and restart.

Scan again,

- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)
- Finding ID: WN11-CC-000170
- Status: **Passed**

Evidence:



Win11BruceNov12DS
VULNERABILITY MANAGEMENT SCANS

WN11-CC-000170 — 1 Results

0 Failed 1 | 0 Warning 1 | 1 Passed 1

1 Item — 1 to 1 of 1 — Page 1 of 1

STATUS	NAME	FAMILY	COUNT
Passed	WN11-CC-000170 - The setting to allow Microsoft accounts to be...	Windows Compliance Checks	1

0 CRITICAL VULNERABILITIES
0 HIGH VULNERABILITIES
0 MEDIUM VULNERABILITIES
0 LOW VULNERABILITIES

Scan Details

STATUS	Completed
START TIME	11/12/2025 at 2:57 PM
TEMPLATE	Advanced Network Scan
SCANNER	LOCAL-SCAN-ENGINE-01

TARGETS
10.1.0.176

---

6. Conclusion

The finding **WN11-CC-000170** 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.