

# 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:

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 > Audit Details'. On the right, there are icons for 'Quick Actions', help, notifications, settings, and a user profile labeled 'BR'. The main heading reads 'WN11-CC-000170 - The setting to allow Microsoft accounts to be optional for modern style apps must be enabled.' Below this, a red 'AUDIT FAILED' badge is visible. The interface is split into two main sections: 'Overview' and 'Assets'. The 'Assets' section contains a search bar and indicates '1 Results'. A table below shows the results with columns for 'STATUS', 'NAME', and 'ACTIONS'. One result is listed with a status of 'FAILED' and a name of '10.1.0.176'. To the right of the table, there is a 'Solution' section with instructions on how to configure the policy value, a 'See Also' link to a download page, and a 'Reference Information' section listing various standards like 800-171, 3.4.2, 800-53, CM-6b, CAT, CCI, CN-1.3, 8.1.10.6(d), CSF2.0, DE.CM-09, PR.PS-01, 800-171R3, 03.04.02a, 800-53R5, CM-6b, CCI, CCI-000366, CSF, PR.IP-1, DISA\_BENCHMARK, and Microsoft\_Windows\_11\_ST.

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

AUDIT FAILED

Overview Assets

Search 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/zlp/U\\_MS\\_Windows\\_11\\_V2R4\\_STIG.zip](https://dl.dod.cyber.mil/wp-content/uploads/stigs/zlp/U_MS_Windows_11_V2R4_STIG.zip)

**Reference Information**

800-171	800-171R3
3.4.2	03.04.02a.
800-53	800-53R5
CM-6b.	CM-6b.
CAT	CCI
III	CCI-000366
CN-1.3	CSF
8.1.10.6(d)	PR.IP-1
CSF2.0	DISA_BENCHMARK
DE.CM-09, PR.PS-01	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:

The screenshot displays the Tenable Vulnerability Management interface. At the top, the header shows 'tenable Vulnerability Management' and a breadcrumb trail 'Scans > Scan Details'. A 'Quick Actions' dropdown is visible. The main content area is titled 'Win11BruceNov12DS' with a sub-header 'VULNERABILITY MANAGEMENT SCANS'. Below this, there are tabs for 'Vulns by Plugin', 'Audits', 'Vulns by Asset', and 'History'. A search bar contains 'WN11-CC-000170' and shows '1 Results'. A summary bar indicates '0 Failed', '0 Warning', and '1 Passed'. A table lists the scan results:

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

On the right, a 'Scan Details' sidebar shows: STATUS: Completed, START TIME: 11/12/2025 at 2:19 PM, TEMPLATE: Advanced Network Scan, SCANNER: LOCAL-SCAN-ENGINE-01, and TARGETS: 10.1.0.176. 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.
- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)
- Finding ID: WN11-CC-000170

Status: **Failed**, Non-Compliant

## Evidence:

The screenshot shows the Tenable Vulnerability Management interface. The top navigation bar includes the Tenable logo, 'Vulnerability Management', and 'Scans > Scan Details'. A search bar at the top right contains 'Win11BruceNov12DS'. Below the search bar, there are tabs for 'Vulns by Plugin', 'Audits', 'Vulns by Asset', and 'History'. The 'Audits' tab is selected, showing a search for 'WN11-CC-000170' with 1 result. A summary bar indicates 1 Failed, 0 Warning, and 0 Passed. Below this, a table lists the audit item: 'Failed' status, 'WN11-CC-000170 - The setting to allow Microsoft accounts to be...' name, 'Windows Compliance Checks' family, and a count of 1. On the right, a 'Scan Details' panel shows the status as 'Completed', start time as '11/12/2025 at 2:35 PM', template as 'Advanced Network Scan', scanner as 'LOCAL-SCAN-ENGINE-01', and targets as '10.1.0.176'. A 'Quick Actions' dropdown is visible in the top right corner.

## 5. Remediation with PowerShell Script

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

The screenshot shows a Windows PowerShell ISE window titled 'Administrator: Windows PowerShell ISE'. The script file 'Remediate-WN11-CC-000170.ps1' is open. The script content is as follows:

```
# Evidence object
34 [pscustomobject]@{
35   ComputerName = $env:COMPUTERNAME
36   STIG_ID       = $stigid
37   SettingName   = 'Allow Microsoft accounts to be optional (App Runtime)'
38   RegistryPath  = 'HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System'
39   ValueName     = $valueName
40   RequiredValue = $desiredValue
41   ActualValue   = $actualValue
42   ComplianceStatus = $compliant
43   ActionTaken  = $action
44   Timestamp     = Get-Date
45 } | Format-List
```

The command prompt shows the execution of the script: 'PS C:\Users\ThreatHunt> C:\Users\ThreatHunt\Desktop\Remediate-WN11-CC-000170.ps1'. The output is as follows:

```
ComputerName : Win11Bruce
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
```

The status bar at the bottom indicates '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:

The screenshot shows the Tenable Vulnerability Management interface. The top navigation bar includes 'tenable Vulnerability Management' and 'Scans > Scan Details'. The main header shows the asset 'Win11BruceNov12DS' and a search bar with 'WN11-CC-000170' entered, resulting in '1 Results'. The left sidebar has tabs for 'Vulns by Plugin', 'Audits', 'Vulns by Asset', and 'History'. The main content area displays a summary of vulnerability counts: 0 Critical, 0 High, 0 Medium, and 0 Low. Below this, a table shows the scan results for the selected finding.

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

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

- 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.