

# STIG Implementation Report

- **Intern Credit Application For:** Bruce Thornton  
**Date:** 10/18/2025  
**STIG Finding:** WN11-CC-000280
  - **SRG:** [SRG-OS-000373-GPOS-00156](#)  
**Severity:** medium  
**Vulnerability ID:** V-253404 **CCI:** CCI-004895
- 

## 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-000280 "Remote Desktop Services must always prompt a client for passwords upon connection.."

---

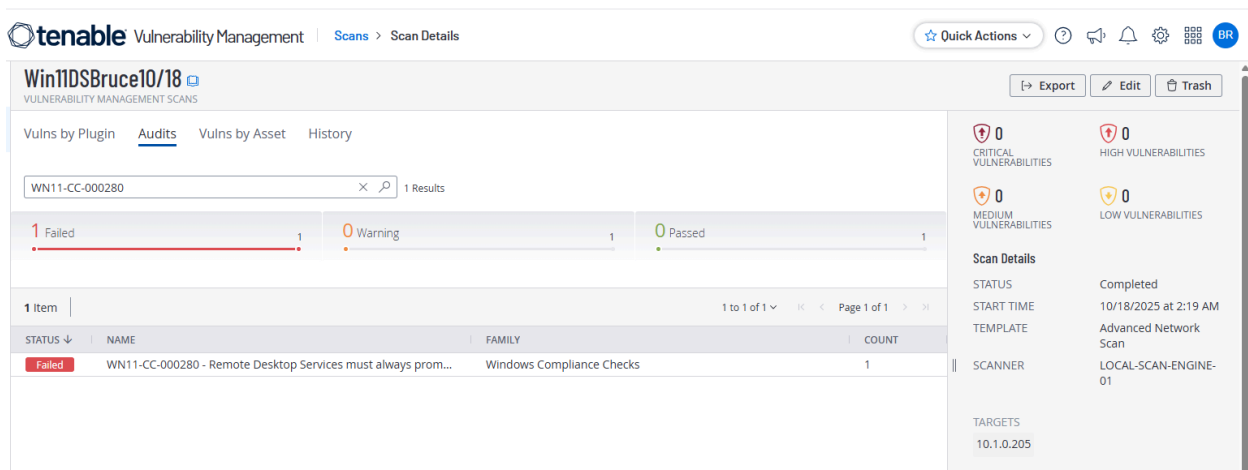
## 2. Initial Scan Results

- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)
- Finding ID: WN11-CC-000280
- Status: **Failed** (non-compliant)

 **Evidence:** First identified the STIG:

<https://stigaview.com/products/win11/v2r1/WN11-CC-000280/>

Initial scan result:



tenable Vulnerability Management | Scans > Scan Details

Win11DSBruce10/18  
VULNERABILITY MANAGEMENT SCANS

[Export] [Edit] [Trash]

Vulns by Plugin Audits Vulns by Asset History

WN11-CC-000280 1 Results

1 Failed 0 Warning 0 Passed

1 Item

STATUS	NAME	FAMILY	COUNT
Failed	WN11-CC-000280 - Remote Desktop Services must always prom...	Windows Compliance Checks	1

Scan Details

STATUS: Completed  
START TIME: 10/18/2025 at 2:19 AM  
TEMPLATE: Advanced Network Scan  
SCANNER: LOCAL-SCAN-ENGINE-01  
TARGETS: 10.1.0.205

### 3. Manual Remediation Steps

Run "gpedit.msc"

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Remote Desktop Services >> Remote Desktop Session Host >> Security >> "Always prompt for password upon connection" to "Enabled".

Run "gpupdate /force" and restart.

Scan again,

- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)
- Finding ID: WN11-CC-000280
- Status: **Passed**

## Evidence:

The screenshot shows the Tenable Vulnerability Management interface for a scan named "Win11DSBruce10/18". The scan is completed and shows 1 Passed result. The interface includes a search bar, a table of results, and a summary of vulnerabilities.

STATUS	NAME	FAMILY	COUNT
Passed	WN11-CC-000280 - Remote Desktop Services must always prom...	Windows Compliance Checks	1

Summary of vulnerabilities:

- CRITICAL VULNERABILITIES: 0
- HIGH VULNERABILITIES: 0
- MEDIUM VULNERABILITIES: 0
- LOW VULNERABILITIES: 0

Scan Details:

- STATUS: Completed
- START TIME: 10/18/2025 at 2:44 AM
- TEMPLATE: Advanced Network Scan
- SCANNER: LOCAL-SCAN-ENGINE-01
- TARGETS: 10.1.0.205

## 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 for a scan named "Win11VMBruce". The scan is completed and shows 1 Failed result. The interface includes a search bar, a table of results, and a summary of vulnerabilities.

STATUS	NAME	FAMILY	COUNT
Failed	WN11-CC-000280 - Remote Desktop Services must always prom...	Windows Compliance Checks	1

Summary of vulnerabilities:

- CRITICAL VULNERABILITIES: 0
- HIGH VULNERABILITIES: 0
- MEDIUM VULNERABILITIES: 0
- LOW VULNERABILITIES: 0

Scan Details:

- STATUS: Completed
- START TIME: 10/18/2025 at 3:17 AM
- TEMPLATE: Advanced Network Scan
- SCANNER: LOCAL-SCAN-ENGINE-01
- TARGETS: 10.1.0.205

## 5. Remediation with PowerShell Script

Utilizing PowerShell ISE.

Save as Remediate-WN11-CC-000280.ps1 (or the name of choice) and run as Administrator:

```
<#
```

```
.SYNOPSIS
```

```
Remediates STIG WN11-CC-000280:
```

```
Forces RDP to always prompt for a password upon connection.
```

```
.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\Windows NT\Terminal Services"
```

```
$RegName = "fPromptForPassword"
```

```
$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 "✅ RDP will always prompt for a password upon connection."
```

```
} else {
```

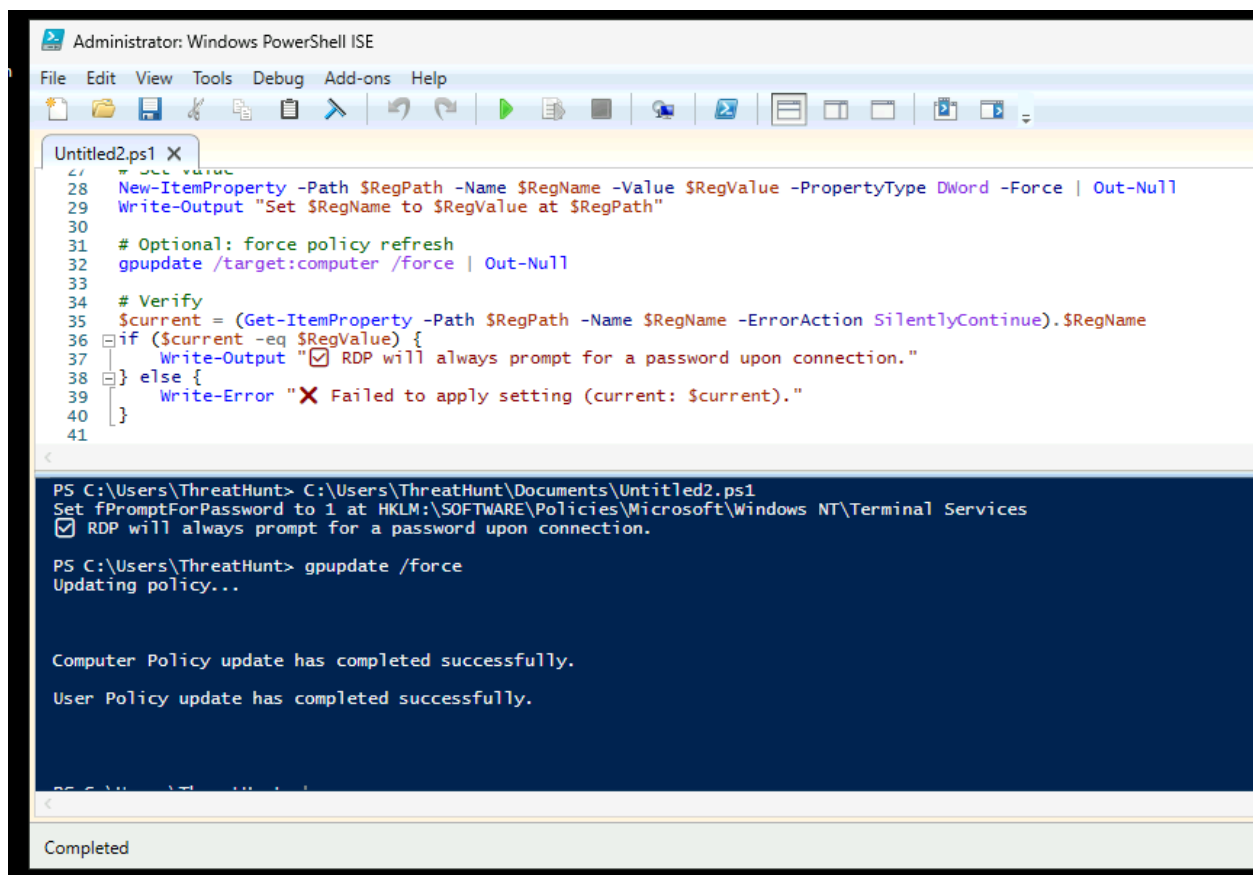
```
    Write-Error "❌ Failed to apply setting (current: $current)."
```

```
}
```

## Notes for Tenable/Nessus

- This control is computer-scope (HKLM under Policies), which Tenable expects.
- After running, do a `gpupdate /force` (script does this) and, if needed, reboot before rescanning.

Saved and ran on Virtual Machine following directions:



The screenshot shows the Windows PowerShell ISE interface. The script in the editor is as follows:

```
27 # Set Value
28 New-ItemProperty -Path $RegPath -Name $RegName -Value $RegValue -PropertyType DWord -Force | Out-Null
29 Write-Output "Set $RegName to $RegValue at $RegPath"
30
31 # Optional: force policy refresh
32 gpupdate /target:computer /force | Out-Null
33
34 # Verify
35 $current = (Get-ItemProperty -Path $RegPath -Name $RegName -ErrorAction SilentlyContinue).$RegName
36 if ($current -eq $RegValue) {
37     Write-Output "☑ RDP will always prompt for a password upon connection."
38 } else {
39     Write-Error "❌ Failed to apply setting (current: $current)."
40 }
41
```

The console output shows the following commands and results:

```
PS C:\Users\ThreatHunt> C:\Users\ThreatHunt\Documents\Untitled2.ps1
Set fPromptForPassword to 1 at HKLM:\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services
☑ RDP will always prompt for a password upon connection.

PS C:\Users\ThreatHunt> gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.

PS C:\Users\ThreatHunt>
```

The status bar at the bottom indicates "Completed".

Ran `"gpupdate /force"` and rescanned.

Status:**Passed**

## Evidence:

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 'Win11VMBruce' and a 'VULNERABILITY MANAGEMENT SCANS' subtitle. Below this, there are tabs for 'Vulns by Plugin', 'Audits' (which is selected), 'Vulns by Asset', and 'History'. A search bar contains the identifier 'WN11-CC-000280' and indicates '1 Results'. A summary bar shows the status counts: 0 Failed, 0 Warning, and 1 Passed. Below this is a table with one item. The table has columns for STATUS, NAME, FAMILY, and COUNT. The single row shows a 'Passed' status for the finding 'WN11-CC-000280 - Remote Desktop Services must always prom...', which belongs to the 'Windows Compliance Checks' family, with a count of 1. On the right side, there are summary cards for vulnerability counts: 0 Critical, 0 High, 0 Medium, and 0 Low. Below these is a 'Scan Details' section with fields for STATUS (Completed), START TIME (10/18/2025 at 9:41 AM), TEMPLATE (Advanced Network Scan), SCANNER (LOCAL-SCAN-ENGINE-01), and TARGETS (10.1.0.205).

STATUS	NAME	FAMILY	COUNT
Passed	WN11-CC-000280 - Remote Desktop Services must always prom...	Windows Compliance Checks	1

## 6. Conclusion

The finding **WN11-CC-000280** 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.