

# Vulnerability Remediation

STIG ID: **WN10-AC-000005**

Severity: **Medium**

CCI: **CCI-002238**

Vuln-ID: **V-220739**

## Vulnerability Discussion

The account lockout feature, when enabled, prevents brute-force password attacks on the system. This parameter specifies the amount of time that an account will remain locked after the specified number of failed logon attempts.

## Verify

Verify the effective setting in Local Group Policy Editor >> Run "gpedit.msc".

Navigate to Local Computer Policy >> Computer Configuration >> Windows Settings >> Security Settings >> Account Policies >> Account Lockout Policy.

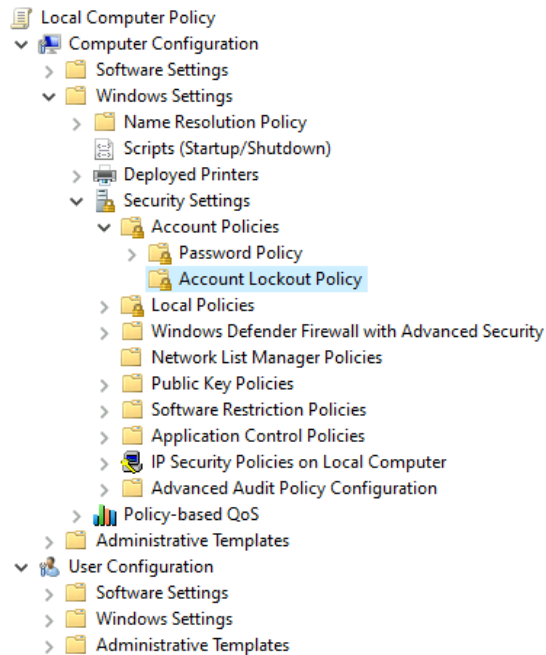
If the "Account lockout duration" is less than "15" minutes (excluding "0"), this is a finding.

Configuring this to "0", requiring an administrator to unlock the account, is more restrictive and is not a finding.

## Remediation - Manual

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Account Policies >> Account Lockout Policy >> "Account lockout duration" to "15" minutes or greater.

A value of "0" is also acceptable, requiring an administrator to unlock the account.



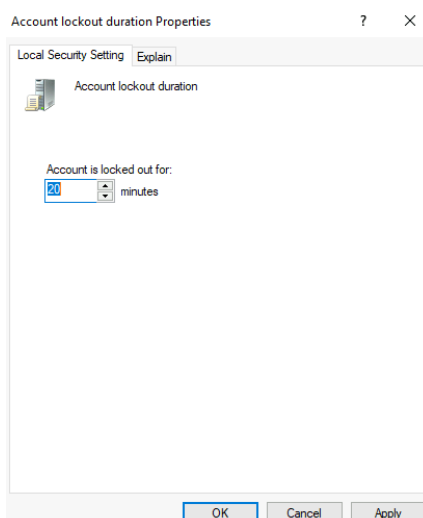
#### Policy

- Account lockout duration
- Account lockout threshold
- Allow Administrator account lockout
- Reset account lockout counter after

#### Security Setting

- 10 minutes
- 10 invalid logon attempts
- Enabled
- 10 minutes

Right Click on “Account lockout duration” >> Click “properties” under the “Local Security Settings” Tab, increase the minutes to 15 or greater or set it to “0”. >> Click “Apply” click “OK”



## Remediation - Programmatic using PowerShell

We'll use `net accounts` to configure the Account Lockout Duration system-wide.

`net accounts /lockoutduration:15` → sets to 15 minutes.

`net accounts /lockoutduration:0` → sets to admin unlock only.

We'll also verify and log the setting after applying.

```
<#
.SYNOPSIS
Remediates STIG ID WN10-AC-000005 (Account Lockout Duration)

.DESCRIPTION
Configures the local security policy "Account lockout duration" to meet STIG compliance (≥15 minutes
or 0).
#>

# Define desired lockout duration (minutes)
$DesiredDuration = 15 # Change to 0 if using admin-unlock policy

Write-Host "Checking current Account Lockout Duration..." -ForegroundColor Cyan
$currentDuration = (net accounts | Select-String "Lockout duration").ToString().Split(":")[1].Trim().Split("
")[0]

Write-Host "Current Lockout Duration: $currentDuration minutes"

if ([int]$currentDuration -lt $DesiredDuration -and [int]$currentDuration -ne 0) {
    Write-Host "Updating Account Lockout Duration to $DesiredDuration minutes..." -ForegroundColor
    Yellow
    net accounts /lockoutduration:$DesiredDuration | Out-Null
    Start-Sleep -Seconds 2
    Write-Host "Lockout duration successfully updated." -ForegroundColor Green
} elseif ([int]$currentDuration -eq 0) {
    Write-Host "Lockout duration is set to 0 (administrator unlock). This is acceptable per STIG."
    -ForegroundColor Green
} else {
    Write-Host "Lockout duration already meets or exceeds STIG requirement." -ForegroundColor Green
}

# Verify the change
Write-Host "`nVerifying current settings..." -ForegroundColor Cyan
net accounts | Select-String "Lockout duration"
Write-Host "`nSTIG WN10-AC-000005 compliance check complete." -ForegroundColor Green
```

Save the script as any name you choose “WIN10-AC-000005.ps1” for example.

Open Powershell as administrator: Run the script .\WIN10-AC-000005.ps1

You should receive the following message to confirm:

```
PS C:\Windows\system32> C:\Users\admin2040\Desktop\WN10-AC-000005.ps1
Checking current Account Lockout Duration...
Current Lockout Duration: 5 minutes
Updating Account Lockout Duration to 15 minutes...
Lockout duration successfully updated.





Verifying current settings...

Lockout duration (minutes): 15

STIG WN10-AC-000005 compliance check complete.

PS C:\Windows\system32>
```

To confirm check the Group Policy:

Policy	Security Setting
 Account lockout duration	15 minutes
 Account lockout threshold	10 invalid logon attempts
 Allow Administrator account lockout	Enabled
 Reset account lockout counter after	5 minutes