# AC.L2-3.1.8

Access Control

## Unsuccessful Logon Attempts

*"Limit unsuccessful logon attempts."*

## Objectives

**[a]**

The means of limiting unsuccessful logon attempts is defined.

**[b]**

The defined means of limiting unsuccessful logon attempts is implemented.

### Key Discussion Points

**Define the Means:**
[a] requires defining the specific mechanism — lockout threshold, lockout duration, and whether reset is manual or automatic must all be documented.

**Lockout vs. Delay:**
v2.13 explicitly permits a delay algorithm as an alternative to hard lockout — either satisfies the control if defined and implemented consistently.

**Applies Everywhere:**
The policy must apply to all access points — workstations, VPN, web portals, remote desktop, and applications. Partial coverage leaves open attack surfaces.

**SIEM Alert Pairing:**
Account lockout stops automated attacks but doesn't detect them. Alert rules on repeated failures allow the security team to identify and investigate credential attacks in progress.

## Assessment Methods

### EXAMINE

Access control policy; procedures addressing unsuccessful logon attempts; system security plan; system design documentation; system configuration settings and associated documentation; system audit logs and records.

### INTERVIEW

Personnel with information security responsibilities; system developers; system or network administrators.

### TEST

Mechanisms implementing access control policy for unsuccessful logon attempts.

# AC.L2-3.1.8

**ACCESS CONTROL — Unsuccessful Logon Attempts**

## Plain English

### What this control is really saying:

A brute force attack is just automated password guessing — and if a system allows unlimited login attempts, an attacker with a word list and time will eventually get in. Account lockout stops this by cutting off attempts after a defined threshold. The threshold, the lockout duration, and where the policy applies must all be defined and implemented.

### How it is used:

- Group Policy sets account lockout at 5 failed attempts, lockout duration of 30 minutes, and observation window of 30 minutes — applied to all domain accounts.
- The same lockout threshold is configured on the VPN concentrator and all web-based portals using the same AD credentials.
- SIEM alerts trigger when more than 10 failed attempts occur against any single account within five minutes — indicating a potential attack.
- Remote Desktop connections are subject to the same lockout policy as local logons — the policy is verified by quarterly configuration review.

## Real World Example

### The Scenario

Acme Defense has a Windows Active Directory environment and a Cisco AnyConnect VPN for remote access. They also use a web-based project management portal that connects to their prime contractor's systems.

### What the assessor finds

The AD Group Policy has no account lockout configured. The web portal has no lockout — an attacker ran a credential spray against it over three days without triggering any alert. The VPN accepts unlimited authentication attempts. All three entry points allow unlimited password guessing.

## SPRS Score Impact

3.1.1 carries a point value of 1. An acceptable use policy without monitoring is unenforceable — and monitoring without a defined authorized use baseline cannot reliably distinguish authorized from unauthorized activity.

## What Good Looks Like

Lockout policy defined with threshold, duration, and observation window, applied to all systems including VPN and web portals, SIEM alerting on repeated failures, policy tested and verified quarterly, lockout applies to both local and network logon attempts.

## Common Gaps

### What assessors actually find in the field:

**✗ No lockout policy**

No account lockout is configured — unlimited login attempts are permitted on workstations, servers, and the VPN.

**✗ Lockout on some systems only**

AD has a lockout policy but the VPN, web portals, and legacy applications do not — these entry points allow unlimited password guessing.

**✗ Threshold too high**

Lockout is configured at 999 failed attempts — effectively unlimited and providing no meaningful protection against brute force.

**✗ Policy exists but untested**

A lockout policy is defined in Group Policy but has never been tested — the configuration may not be functioning as intended.

**✗ No alerting on failed attempts**

Failed logon attempts are logged but no alerts are configured — credential spray attacks generate no notifications and go undetected.