AC.L2-3.1.11

Access Control

Session Termination

"Terminate (automatically) a user session after a defined condition."

Objectives

[a]

Conditions requiring a user session to terminate are defined.

[b]

A user session is automatically terminated after any of the defined conditions occur.

Key Discussion Points

Lock vs. Terminate:
Session lock (3.1.10) pauses a session — session termination (3.1.11) ends it entirely and requires full re-authentication. Both are required; they address different threat scenarios.

Token Invalidation:
Web application session termination must invalidate the session token — closing a browser tab without server-side invalidation leaves the token exploitable.

Define the Conditions:
[a] requires documenting the specific conditions — inactivity period, time-of-day cutoff, policy violation triggers. Without defined conditions, [b] cannot be evaluated.

Remote Sessions Critical:
VPN, RDP, and SSH sessions that persist indefinitely are a primary attack surface — long-lived remote sessions provide extended windows for lateral movement after initial compromise.

Assessment Methods

EXAMINE

Access control policy; procedures addressing session termination; system design documentation; system security plan; system configuration settings and associated documentation; list of conditions or trigger events requiring session disconnect; system audit logs and records.

INTERVIEW

System or network administrators; personnel with information security responsibilities; system developers.

TEST

Mechanisms implementing user session termination.

AC.L2-3.1.11

ACCESS CONTROL — Session Termination

Plain English

What this control is really saying:

Session lock pauses a session — session termination ends it entirely and requires a full re-login. This control requires defining the conditions under which sessions must be terminated (inactivity timeout, end of workday, policy violation, maintenance window) and configuring systems to enforce those terminations automatically. An idle VPN connection or web session that persists for days is a session termination gap.

How it is used:

- The SSP documents session termination conditions: VPN sessions terminate after 4 hours of inactivity; web portal sessions expire after 30 minutes; RDP sessions terminate after 60 minutes.
- VPN concentrator is configured with an inactivity timeout that terminates the session and invalidates the session token — re-authentication is required to reconnect.
- Web application sessions invalidate the session token on expiration — users cannot resume an expired session by pressing the back button.
- Conditions for termination are defined in policy and include inactivity timeout, end of authorized maintenance window, and detection of a defined policy violation.

Real World Example

The Scenario

Acme Defense uses a web-based project management portal accessed by engineers and their prime contractor. Engineers also connect via Cisco AnyConnect VPN for remote access to the CUI file server.

What the assessor finds

The web portal has no session expiration configured. Users who authenticated last Monday are still active in the system. VPN sessions have a 24-hour maximum but no inactivity timeout — a laptop left in sleep mode at home remains connected to the CUI environment. No termination conditions are documented in the SSP.

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

Session termination conditions documented in SSP, VPN inactivity timeout configured, web sessions expire with token invalidation after defined period, RDP sessions terminate rather than lock, conditions cover inactivity, end of day, and policy violations.

Common Gaps

What assessors actually find in the field:

✗ **No termination conditions defined**

The organization has never documented what conditions require session termination — [a] is not met and automatic termination cannot be evaluated without it.

✗ **VPN sessions never terminate**

VPN sessions remain active indefinitely with no inactivity timeout — a connected session from a compromised device stays open without limit.

✗ **Web sessions persist**

Web application sessions do not expire — users authenticated days ago remain active and their session tokens remain valid.

✗ **Lock only, no termination**

Sessions lock after inactivity but are never terminated — the session token remains valid and can be resumed without full re-authentication.

✗ **Remote sessions left open**

RDP and SSH sessions are routinely left connected overnight with no automatic termination — long-lived sessions expand the window for lateral movement.