MA.L2-3.7.5

Maintenance

Nonlocal Maintenance

"Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete."

Objectives

[a]

Multifactor authentication is used to establish nonlocal maintenance sessions via external network connections.

[b]

Nonlocal maintenance sessions established via external network connections are terminated when nonlocal maintenance is complete.

Key Discussion Points

MFA Required:
Any remote maintenance session over an external network requires MFA — password-only remote admin access is a direct finding.

Terminate When Done:
When the work is complete, the session must be closed — persistent remote connections that stay open after maintenance are a gap.

Reflects IA.L2-3.5.3:
3.7.5 applies the same MFA requirement from 3.5.3 specifically to remote maintenance — an explicit extension of that control.

Nonlocal Defined:
Nonlocal means over an external network — MSP VPN, vendor remote desktop, or cloud console all qualify. Local keyboard access does not.

Assessment Methods

EXAMINE

System maintenance policy; procedures addressing nonlocal system maintenance; system security plan; system design documentation; system configuration settings; maintenance records; diagnostic records.

INTERVIEW

Personnel with system maintenance responsibilities; personnel with information security responsibilities; system or network administrators.

TEST

Organizational processes for managing nonlocal maintenance; mechanisms implementing and supporting nonlocal maintenance; mechanisms for strong authentication of nonlocal maintenance sessions; mechanisms for terminating sessions.

MA.L2-3.7.5

MAINTENANCE — Nonlocal Maintenance

Plain English

What this control is really saying:

Your MSP connects to your server via RDP to apply patches. If that connection only requires a username and password, a stolen credential gives an attacker full remote access to your CUI systems. This control requires MFA on every nonlocal maintenance session and mandates that the session is closed when the work is done.

How it is used:

- The MSP VPN requires both a password and a hardware token — no remote maintenance session can begin without both factors successfully presented.
- MSP technicians acknowledge in the session log when they initiate and terminate each remote session — open sessions are reviewed and closed daily.
- The firewall is configured to terminate inactive remote maintenance sessions after 30 minutes — automatic timeout prevents sessions from persisting.
- MFA for nonlocal maintenance is documented in the SSP — the authentication method, session timeout policy, and termination procedure are all specified.

Real World Example

The Scenario

Acme Defense's MSP manages servers remotely via RDP. The MSP admin account uses only a password for authentication. An MSP technician connected last Tuesday for a patch job — the session is still open six days later.

What the assessor finds

No MFA is configured for any remote maintenance access. The open six-day session has admin rights to all CUI systems. No session timeout exists. If the MSP technician's credentials were compromised at any point this week, an attacker has had persistent admin access.

SPRS Score Impact

3.7.5 carries a point value of 3. Unprotected remote maintenance access is one of the primary pathways threat actors use to pivot from MSP networks into DIB contractor environments.

What Good Looks Like

MFA enforced for all nonlocal maintenance sessions, sessions terminated when work is complete, session timeout configured, session start and stop logged, MFA method and termination procedure documented in SSP.

Common Gaps

What assessors actually find in the field:

✗ **Remote admin with password only**

The MSP connects via RDP using only a username and password — MFA is not configured for remote maintenance access.

✗ **Session never terminated**

The MSP's remote session has been continuously connected for three weeks — nobody logged out when the maintenance work finished.

✗ **MFA on VPN but not console**

VPN access requires MFA but the server management console is accessible with only a password once on the network.

✗ **No session logging**

Remote maintenance sessions are not logged — there is no record of when sessions were opened, what was done, or when they closed.

✗ **Auto-timeout not configured**

No session timeout is set — an authenticated remote session will remain open indefinitely if the technician walks away.