IA.L2-3.5.3

Identification & Authentication

Multifactor Authentication

"Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts."

Objectives

[a]
Privileged accounts are identified.

[b]
Multifactor authentication is implemented for local access to privileged accounts.

[c]
Multifactor authentication is implemented for network access to privileged accounts.

[d]
Multifactor authentication is implemented for network access to non-privileged accounts.

Key Discussion Points

The Three Factors:
Something you know (password/PIN), something you have (token/smart card), something you are (biometric) — any two required.

Local AND Network:
Privileged accounts need MFA for both local login and network access. Non-privileged accounts need MFA for network access only.

Mobile Devices Count:
If a mobile device accesses a CUI system or application, MFA is required — no exceptions for phones or tablets.

5-Point Control:
3.5.3 carries the highest SPRS weight in IA — missing MFA on privileged accounts is one of the most expensive single gaps.

Assessment Methods

EXAMINE

Identification and authentication policy; procedures addressing user identification and authentication; system security plan; system design documentation; system configuration settings; system audit logs; list of system accounts.

INTERVIEW

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

TEST

Mechanisms supporting or implementing authenticator management capability.

Plain English

What this control is really saying:

A password alone can be stolen, guessed, or phished. MFA requires a second factor that an attacker is unlikely to also possess — a code from an app, a hardware token, or a fingerprint. This control mandates MFA for all privileged access (local and remote) and for all non-privileged network access. Password-only is not sufficient.

How it is used:

- All admin accounts require MFA for both local logon and network access — enforced via Microsoft Authenticator app and Conditional Access policy.
- All standard users accessing CUI systems over VPN require MFA — the VPN is integrated with Azure AD and pushes an MFA prompt at each connection.
- Cloud-based email and SharePoint require MFA for all users — Conditional Access blocks access without a valid MFA session.
- MFA is documented in the SSP with the method (TOTP app), scope (all accounts), and enforcement mechanism (Azure AD Conditional Access).

IA.L2-3.5.3

IDENTIFICATION & AUTHENTICATION — Multifactor Authentication

Real World Example

The Scenario

Acme Defense uses Microsoft 365 for email and file sharing. The IT admin enabled MFA for standard users on the VPN. However, the domain admin account used for server management has MFA disabled — the IT admin found it inconvenient during maintenance windows.

What the assessor finds

The domain admin account authenticates with only a password for both local and network access — [b] and [c] are not met. The M365 tenant has no Conditional Access policy — admin portal access is password-only. Legacy auth protocols are not blocked.

SPRS Score Impact

3.5.3 carries a point value of 5. Missing MFA on privileged accounts is one of the highest-value single gaps in the entire SPRS scoring model — and the most commonly exploited path in DIB intrusions.

What Good Looks Like

MFA enforced on all privileged accounts for local and network access, MFA enforced on all non-privileged accounts for network/VPN access, cloud apps covered by Conditional Access, legacy auth blocked, MFA method and scope documented in SSP.

Common Gaps

What assessors actually find in the field:

✗ **No MFA on VPN**

Remote access only requires a username and password — a phished credential gives an attacker full network access.

✗ **Admin accounts exempt from MFA**

Standard users have MFA but admin accounts were excluded 'for convenience' — the highest-risk accounts are the least protected.

✗ **MFA only for remote, not local**

MFA is enforced on VPN but privileged accounts can log in locally with just a password — [b] is not met.

✗ **Cloud apps without MFA**

Microsoft 365 and SharePoint are accessible with a password only — no Conditional Access or MFA policy is configured.

✗ **MFA bypassable**

MFA is configured but legacy authentication protocols (SMTP, IMAP) are not blocked — attackers can bypass MFA entirely.