IA.L2-3.5.2

Identification & Authentication

Authentication [CUI Data]

"Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems."

Objectives

[a]
The identity of each user is authenticated or verified as a prerequisite to system access.

[b]
The identity of each process acting on behalf of a user is authenticated or verified as a prerequisite to system access.

[c]
The identity of each device accessing or connecting to the system is authenticated or verified as a prerequisite to system access.

Key Discussion Points

Change Defaults:
Default credentials on any device are a direct finding — change every default username and password before deployment, no exceptions.

All Three Categories:
Users, processes, and devices all require authentication — a service account with no password or a device with no cert is a gap.

Authenticator Types:
Passwords, key cards, cryptographic devices, and one-time tokens all qualify — the type must match the risk and system requirements.

Temp Authenticators:
Credentials issued for temporary access must be revoked when no longer needed — vendor accounts that persist are a finding.

Assessment Methods

EXAMINE

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

INTERVIEW

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

TEST

Mechanisms supporting or implementing authenticator management capability.

IA.L2-3.5.2

IDENTIFICATION & AUTHENTICATION — Authentication [CUI Data]

Plain English

What this control is really saying:

Identification (3.5.1) says who you are. Authentication (3.5.2) proves it. A username without a password, a device without a certificate, or a service account with no credential — none of those are authenticated. This control requires that access to CUI systems is gated by verified identity, not just claimed identity.

How it is used:

- All users authenticate with a unique username and password meeting the organization's complexity requirements before accessing any CUI system.
- All network devices (firewall, switches, access points) have their default credentials changed before deployment — documented in the change record.
- Service accounts authenticate using unique passwords stored in a password vault — no service runs without a credential.
- Remote maintenance sessions require authentication via individual credentials — temporary accounts are disabled within 24 hours of session end.

Real World Example

The Scenario

Acme Defense deployed a new managed switch last quarter. The IT admin never changed the default admin credentials. A firewall was also installed using the vendor's default username 'admin' and password 'admin' — both are still active.

What the assessor finds

Both devices are accessible with publicly documented default credentials. A Google search for the switch model returns the default password in under 30 seconds. No device authentication policy exists and no default credential change procedure is documented.

SPRS Score Impact

3.5.2 carries a point value of 1. Though low-weighted, identification is the prerequisite for every other IA control — without unique identities for users, processes, and devices, authentication and access control are meaningless.

What Good Looks Like

All users authenticate before access, default credentials changed on all devices, service accounts require credentials, device authentication enforced where feasible, temp credentials tracked and revoked, auth methods documented in SSP.

Common Gaps

What assessors actually find in the field:

✗ Default passwords not changed

Routers, switches, and servers deployed with factory default credentials — widely known and easily exploited.

✗ Service accounts with no auth

Scheduled tasks and backup agents run without credentials or use blank passwords — no authentication gate.

✗ Device auth not implemented

Workstations connect to the domain without device certificates — only user credentials are verified, not the device.

✗ Temp credentials not revoked

Vendor accounts created for on-site work are still active months after the visit — permanent backdoor.

✗ Unauthenticated guest WiFi

Guest wireless in the office has no authentication and is on the same network segment as CUI systems.