IA.L2-3.5.7

Identification & Authentication

Password Complexity

"Enforce a minimum password complexity and change of characters when new passwords are created."

Objectives

[a]
Password complexity requirements are defined.

[b]
Password change of character requirements are defined.

[c]
Minimum password complexity requirements as defined are enforced when new passwords are created.

[d]
Minimum password change of character requirements as defined are enforced when new passwords are created.

Key Discussion Points

Two Requirements:
This control covers two things: complexity (character types and length) AND change of characters (minimum changed from prior password).

Organization Defines:
NIST leaves the specific minimums to the organization — but you must define them, document them, and enforce them technically.

Technically Enforced:
Complexity rules must be enforced by the system — Group Policy, IAM platform, or application — not just stated in policy.

Applies to All Passwords:
This applies to single-factor and the password component of MFA authenticators — no accounts are exempt.

Assessment Methods

EXAMINE

Identification and authentication policy; password policy; procedures addressing authenticator management; system security plan; system configuration settings; system design documentation; password configurations and associated documentation.

INTERVIEW

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

TEST

Mechanisms supporting or implementing authenticator management capability.

IA.L2-3.5.7

IDENTIFICATION & AUTHENTICATION — Password Complexity

Plain English

What this control is really saying:

Weak passwords are cracked. This control requires that you define what a strong password looks like — minimum length, required character types, and how many characters must change when a password is updated — and then make the system enforce those rules. Policy without technical enforcement is not sufficient.

How it is used:

- Password policy requires: minimum 12 characters, at least one uppercase, one lowercase, one number, and one special character.
- Password change requirement: minimum 4 characters must differ from the previous password — enforced via Active Directory Fine-Grained Password Policy.
- Group Policy Object applies the password complexity settings to all domain-joined systems — noncompliant passwords are rejected at the time of creation.
- Password requirements are documented in the SSP and in the acceptable use policy — users are trained on the requirements during onboarding.

Real World Example

The Scenario

Acme Defense's Active Directory has the default Windows password policy: 7-character minimum, complexity enabled. No fine-grained policy is in place. The IT admin is unaware that 'complexity enabled' in Windows only requires one category change — it does not enforce a mix of all four character types.

What the assessor finds

Users have passwords like 'Acme2024!' that technically pass Windows complexity but use only 9 characters and a predictable pattern. No change-of-character requirement exists. The organization believes the policy is adequate but has never formally defined the minimums in the SSP.

SPRS Score Impact

3.5.7 carries a point value of 5. Weak or predictable passwords are the easiest credential to attack — and undefined or unenforced complexity requirements mean users will always gravitate toward the path of least resistance.

What Good Looks Like

Complexity requirements formally defined (minimum length, required character types), change of character requirement defined, both enforced technically via GPO or IAM, requirements documented in SSP and password policy, all account types covered.

Common Gaps

What assessors actually find in the field:

✗ No complexity requirements

The organization has no documented password complexity policy — users set any password they choose.

✗ Policy not technically enforced

A complexity requirement is stated in policy but Group Policy is not configured — users can still set weak passwords.

✗ No change of character rule

Complexity is enforced but there is no requirement to change a minimum number of characters — users rotate between 'Password1!' and 'Password2!'.

✗ Short minimum length

Password policy requires only 6 characters — far below current guidance and easily brute-forced.

✗ Some systems not covered

Domain accounts have complexity requirements but local accounts and application accounts have no policy applied.