IA.L2-3.5.8

Identification & Authentication

Password Reuse

"Prohibit password reuse for a specified number of generations."

Objectives

[a]

The number of generations during which a password cannot be reused is specified.

[b]

Reuse of passwords is prohibited during the specified number of generations.

Key Discussion Points

Define Generations:
You must specify how many previous passwords cannot be reused — 5 to 24 generations is common practice.

Temp Passwords Exempt:
The guide explicitly states that password lifetime restrictions do not apply to temporary passwords — only regular account passwords.

Works With Complexity:
3.5.8 is designed to work with 3.5.7 — complexity makes each password hard to guess; reuse prohibition forces genuinely new passwords.

Technically Enforced:
Group Policy or IAM must store and compare password history — a policy statement without technical enforcement does not satisfy [b].

Assessment Methods

EXAMINE

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

INTERVIEW

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

TEST

Mechanisms supporting or implementing password-based authenticator management capability.

IA.L2-3.5.8

IDENTIFICATION & AUTHENTICATION — Password Reuse

Plain English

What this control is really saying:

If users can immediately reuse an old password when forced to change, the change requirement means nothing. This control requires that the system remember a defined number of previous passwords and reject any attempt to reuse one of them. Without this, 'Password1!' just cycles back to 'Password1!' after a few changes.

How it is used:

- Active Directory password policy is configured to enforce a password history of 24 generations — the last 24 passwords cannot be reused.
- Users who attempt to reuse a recent password receive an error message and are required to create a unique new password.
- The password history setting is applied via Group Policy to all domain-joined systems and verified quarterly during configuration compliance checks.
- Password reuse prohibition is documented in the SSP and in the acceptable use policy — 24-generation history is the organization's defined standard.

Real World Example

The Scenario

Acme Defense has a password change policy but the AD password history is set to the Windows default of 0 (no history). Users are required to change passwords every 90 days but can immediately reuse their previous password when prompted.

What the assessor finds

Multiple users immediately reset to their previous password when prompted to change. No generations are prohibited — AD history is set to 0. The password policy document mentions 'no reuse' but there is no technical control enforcing it.

SPRS Score Impact

3.5.8 carries a point value of 5. A password change requirement without reuse prohibition is theater — users will always reuse familiar passwords unless technically prevented from doing so.

What Good Looks Like

Number of prohibited generations defined in policy (minimum 5, 24 recommended), AD password history configured to match, all account types covered, reuse attempts rejected by system, requirement documented in SSP and password policy.

Common Gaps

What assessors actually find in the field:

✗ Password history not configured

Active Directory password history is set to 0 — users can immediately reuse their previous password.

✗ Too few generations

Password history is set to 3 — users cycle through three passwords and return to their favorite.

✗ Policy not enforced

The policy states 10 generations but AD password history is not configured — the system does not enforce it.

✗ Some accounts excluded

Service accounts and local admin accounts have no password history requirement — reuse is unrestricted.

✗ Combined with short lifetime

Password reuse prohibition is undermined by a short change interval — users can cycle through the required generations quickly.