

Password Policies, Group Policy, and What NIST Changed

Sat, Aug 8, 6:00 PM EDT · <https://scottslab.io/posts/password-policies-and-group-policy>



TL;DR

Most Active Directory domains still enforce the password rules NIST retired years ago: forced 90-day rotation and character-class complexity, both baked into the Default Domain Policy and never revisited. NIST 800-63B reversed that: length over composition, no routine expiration, and screening against known-bad passwords. The catch is that classic Group Policy only gives you **one** password policy for the whole domain; the fix almost nobody configures is Fine-Grained Password Policies (PSOs), which let you give service accounts, admins, and standard users their own rules. And before you flip anything: dropping rotation will trip your auditor, so bring the 800-63B citation to the meeting.

If you open the Default Domain Policy on a random AD domain, you can usually guess what you'll find before it loads: minimum length 8, complexity enabled, maximum password age 90 days, history of the last few passwords. Those numbers have been the reflex since before most of the domain's users were hired, and nobody has touched them since the domain was stood up. That's the actual problem here, and it's worth being precise about it. This is not a knowledge problem. NIST published the new guidance years ago and everyone's read the headlines. It's a configuration problem. The rules are sitting in a GPO that got set once and never opened again.

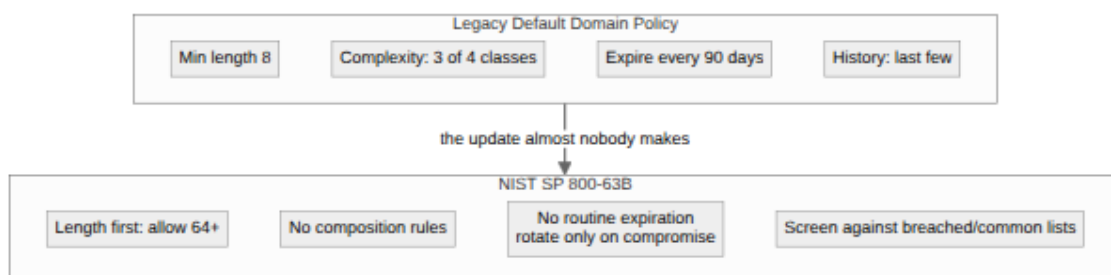
How the policy actually reaches the machine

Password policy in AD is not a document, it's Group Policy, and the delivery has one quirk that shapes everything else. Group Policy in general inherits down the tree: site, then domain, then nested OUs, with the closest object winning. That's why you can hand the Marketing OU a different desktop wallpaper than Finance. Account policy is the exception. The password and lockout settings that apply to domain users are read from the **Default Domain Policy at the domain root**, and linking a stricter password GPO to an OU does nothing for domain accounts. For decades that meant one truth per domain: every user, from the temp who started Monday to the Domain Admin, lived under the same password rule. If you wanted admins on a longer password, your options were a separate domain or a sticky note. That single constraint is why so many environments never tightened anything. There was no clean place to put the exception.

What NIST 800-63B actually says now

The reversal is broader than "make them longer," and the specifics matter because your audience will check them. NIST 800-63B drops the two rituals we defended for years: **no composition rules** (no mandated upper/lower/digit/symbol mix) and **no periodic expiration**: you rotate a password only when there's evidence it was compromised. In their place, the guidance is length-first: a minimum of 8, but verifiers *should* accept at least 64, because the whole point is to let people use a passphrase. Screen every new password against a list of known-compromised and common values, and stop fighting the user in petty ways: allow paste so password managers work, allow the full printable and Unicode range.

The reasoning is the part the old policy got exactly backwards. Forced complexity plus a 90-day clock doesn't produce strong passwords; it produces Summer2026! , then Summer2026!! , then a sticky note on the monitor. It optimized for a form validator, not for an attacker, and an attacker was never slowed by it. Length is what costs a cracker real time; a rotation treadmill just guarantees a predictable pattern.



There's a hardening layer worth stating separately so it isn't confused with NIST: privileged accounts should be held to a higher bar than everyone else. A **15-character minimum** is the common CIS-style recommendation, and it sits naturally on top of the length-first philosophy. But you can't apply "15 for admins, 12 for everyone else" from a single Default Domain Policy. That's the whole reason the next section exists.

Fine-Grained Password Policies: the setting nobody opens

This is the part that surprised me when I first dug in, and in a decade of AD conversations I've found most admins either don't know it exists or have never configured one. **Fine-Grained Password Policies** (implemented as Password Settings Objects, PSOs) have shipped since Windows Server 2008, and they break the one-policy-per-domain rule cleanly. You define a policy object with its own length, complexity, history, age, and lockout values, and you scope it to specific users or groups, all without touching the Default Domain Policy.

They live in a container most people never browse: `CN=Password Settings Container,CN=System` in the domain. The one scoping rule to internalize is that a PSO applies to **users and global security groups only, not OUs**. If you think in OUs, the standard move is a *shadow group*: a security group whose membership mirrors the OU, which you point the PSO at. This is also the moment security groups stop being just a folder-permission tool and become the delivery mechanism for password policy. The same group you use to grant access is the one that carries the rule.

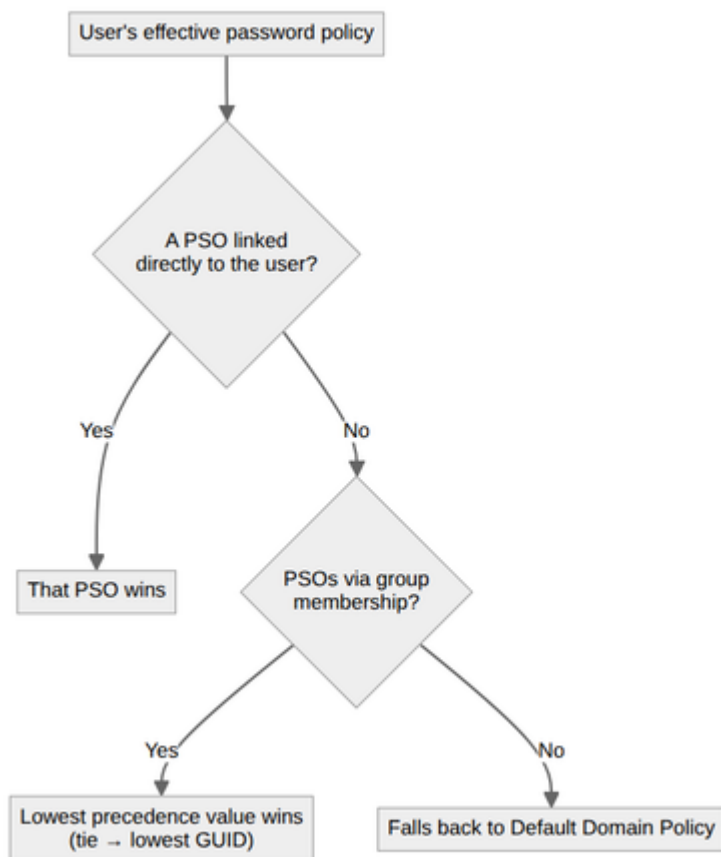
The build is short. In the Active Directory Administrative Center, go to the tree view → System → Password Settings Container → New → Password Settings, fill in the values, and add the target group as a subject. In PowerShell it's two commands:

```
New-ADFineGrainedPasswordPolicy -Name "PS0-Privileged" -Precedence 10 `
  -MinPasswordLength 15 -ComplexityEnabled $false `
  -PasswordHistoryCount 24 -MaxPasswordAge "00:00:00"
Add-ADFineGrainedPasswordPolicySubject -Identity "PS0-Privileged" -Subjects
  "Domain Admins"
```

`-MaxPasswordAge "00:00:00"` is how you implement NIST's no-rotation guidance. Zero means the password never expires on a schedule. So a realistic setup ends up being three PSOs: privileged accounts at 15 characters and no expiry, service accounts at 25+ (they never type it, so make it long), and standard users on a sane length-first default: each targeting its own group, none of them touching the domain policy.

When two policies both apply

The obvious question, and the one an engineer asked me the minute I posted about this: what happens when a user is in two groups that each have a PSO? PSOs resolve by the **msDS-PasswordSettingsPrecedence** value, and **lower wins**. A PSO linked directly to the user beats any group-linked PSO regardless of number. Among group PSOs, the lowest precedence value applies, and if there's a tie, the lowest object GUID breaks it. That's a deterministic-but-arbitrary tiebreaker you never want to actually rely on, so keep your precedence numbers distinct and spaced out (10, 20, 30) rather than clever.



The control that actually kills Summer2026!

Dropping complexity rules only works if something is still stopping genuinely weak passwords, and that something is a banned-password list. **Entra Password Protection** ships a Microsoft-maintained global list of known-bad passwords and lets you add a custom list of your own (your company name, local sports teams, **Summer**, **Winter**, whatever your users actually pick). The piece people miss is that it extends to on-prem AD: you install a DC agent and a proxy service, and the same fuzzy, substring-aware matching that runs in the cloud now rejects **Summer2026!** and **P@ssw0rd** at the domain controller. That's the real answer to "if I drop complexity, won't people pick garbage?" You replace a rule that guessed at strength with one that checks it against reality.

Bring the citation to the audit

Here's the unglamorous part that will actually cost you time. Turning off forced rotation is technically two clicks, but it directly contradicts the questionnaire your cyber-insurance carrier and your auditor are reading from, because those documents were written against the old advice and haven't caught up. If you flip it silently, you'll spend renewal season arguing the point. Pair the change with a one-line note in your control documentation citing NIST SP 800-63B as the basis for removing scheduled expiration, and hand it to your assessor before they ask. It converts a finding into a footnote, and it's the difference between "we're out of compliance" and "we made a deliberate, standards-backed decision."

None of this is the endgame. The endgame is passwordless, and phishing-resistant passkeys make most of this argument moot for the accounts that support them. But you have a domain full of passwords today, and "eventually passwordless" is not a policy. Fix the GPO, add the PSOs, turn on the banned list, and write the note for your auditor. It's a genuinely easy win, which is exactly why it's worth being the one who finally opens the setting nobody has touched in years.

Written by Scott S. — Contact: scott@scottschlangen.com — scottslab.io — <https://scottslab.io/posts/password-policies-and-group-policy>