


NIST Password Guidelines

 blog.netwrix.com/2022/11/14/nist-password-guidelines

What are NIST Password Guidelines?

Since 2014, the National Institute of Standards and Technology (NIST), a U.S. federal agency, has issued guidelines for managing digital identities via Special Publication 800-63B. The latest revision (rev. 3) was released in 2017, and has been updated as recently as 2019. Revision 4 was made available for comment and review; however, revision 3 is still the standard as of the time of this blog post.

Section 5.1.1 – Memorized Secrets provides recommendations for requirements around how users may create new passwords or make password changes, including guidelines around issues such as password strength. Special Publication 800-63B also covers verifiers (software, websites, network directory services, etc.) that validate and handle passwords during authentication and other processes.

Handpicked related content:

[Password Policy Best Practices for Strong Security in AD](#)

Not all organizations must adhere to NIST guidelines. However, many follow NIST password policy recommendations even if it's not required because they provide a good foundation for sound digital identity management. Indeed, strong password security helps companies block many cybersecurity attacks, including hackers, brute force attacks like credential stuffing and dictionary attacks. In addition, mitigating identity-related security risks helps organizations ensure compliance with a wide range of regulations, such as HIPAA, FISMA and SOX.

Quick List of NIST Password Guidelines

This blog explain many NIST password guidelines in detail, but here's a quick list:

- User-generated passwords should be at least 8 characters in length.
- Machine-generated passwords should be at least 6 characters in length.
- Users should be able to create passwords at least 64 characters in length.
- All ASCII/Unicode characters should be allowed, including emojis and spaces.
- Stored passwords should be hashed and salted, and never truncated.
- Prospective passwords should be compared against password breach databases and rejected if there's a match.
- Passwords should not expire.
- Users should be prevented from using sequential characters (e.g., "1234") or repeated characters (e.g., "aaaa").
- Two-factor authentication (2FA) should not use SMS for codes.
- Knowledge-based authentication (KBA), such as "What was the name of your first pet?", should not be used.

- Users should be allowed 10 failed password attempts before being locked out of a system or service.
- Passwords should not have hints.
- Complexity requirements — like requiring special characters, numbers or uppercase letters — should not be used.
- Context-specific words, such as the name of the service or the individual's username, should not be permitted.

You probably notice that some of these recommendations represent a departure from previous assumptions and standards. For example, NIST has removed complexity requirements like special characters in passwords; this change was made in part because users find ways to circumvent stringent complexity requirements. Instead of struggling to remember complex passwords and risking getting locked out, they may write their passwords down and leave them near physical computers or servers. Or they simply recycle old passwords based on dictionary words by making minimal changes during password creation, such as incrementing a number at the end.

NIST Guidelines

Now let's explore the NIST guidelines in more detail.

Password length & processing

Length has long been considered a crucial factor for password security. NIST now recommends a password policy that requires all user-created passwords to be at least 8 characters in length, and all machine-generated passwords to be at least 6 characters in length. Additionally, it's recommended to allow passwords to be at least 64 characters as a maximum length.

Verifiers should no longer truncate any passwords during processing. Passwords should be hashed and salted, with the full password hash stored.

Also the recommended NIST account lockout policy is to allow users at least 10 attempts at entering their password before being locked out.

Accepted characters

All ASCII characters, including the space character, should be supported in passwords. NIST specifies that Unicode characters, such as emojis, should be accepted as well.

Users should be prevented from using sequential characters (e.g., "1234"), repeated characters (e.g., "aaaa") and simple dictionary words.

Commonly used & breached passwords

Passwords that are known to be commonly used or compromised should not be permitted. For example, you should disallow passwords in lists from breaches (such as the [Have I Been Pwned?](#) database, which contains 570+ million passwords from breaches), previously used passwords, well-known commonly used passwords, and context-specific passwords (e.g., the name of the service).

When a user attempts to use a password that fails this check, a message should be displayed asking them for a different password and providing an explanation for why their previous entry was rejected.

Reduced complexity & password expiration

As explained earlier in the blog, previous password complexity requirements have led to [less secure human behavior](#), instead of the intended effect of tightening security. With that in mind, NIST recommends reduced complexity requirements, which includes removing requirements for special characters, numbers, uppercase characters, etc.

A related recommendation for reducing insecure human behavior is to eliminate password expiration.

No more hints or knowledge-based authentication (KBA)

Although password hints were intended to help users to create more complex passwords, users often choose hints that practically give away their passwords. Accordingly, NIST recommends not allowing password hints.

NIST also recommends not using knowledge-based authentication (KBA), such as questions like “What was the name of your first pet?”

Password managers & two-factor authentication (2FA)

To account for the growing popularity of password managers, users should be able to paste passwords.

SMS is no longer considered a secure option for 2FA. Instead, one-time code provider, such as Google Authenticator or Okta Verify, should be used.

How Netwrix Can Help

Netwrix offers several solutions specifically designed to streamline and strengthen access and password management:

- [Netwrix Password Policy Enforcer](#) makes it easy to create strong yet flexible password policies that enhance security and compliance without hurting user productivity or burdening helpdesk and IT teams.

- Netwrix Password Reset enables users to safely unlock their own accounts and reset or change their own passwords, right from their web browser. This self-service functionality dramatically reduces user frustration and productivity losses while slashing helpdesk call volume.

FAQ

What is NIST Special Publication 800-63B?

NIST's Digital Identity Guidelines (Special Publication 800-63B) provides reliable recommendations for identity and access management, including effective password policies.

Why does NIST recommend reducing password complexity requirements?

While requiring complex passwords makes them more difficult for attackers to crack, it also makes passwords harder for users to remember. To avoid frustrating lockouts, users tend to respond with behaviors like writing down their credentials on a sticky note by their desk or choosing to periodically reuse the same (or nearly the same) password — which increase security risks. Accordingly, NIST now recommends less stringent complexity requirements.

Joe Dibley

Security Researcher at Netwrix and member of the Netwrix Security Research Team. Joe is an expert in Active Directory, Windows, and a wide variety of enterprise software platforms and technologies, Joe researches new security risks, complex attack techniques, and associated mitigations and detections.

