ManageEngine
ADSelfService Plus

# NIST password guidelines Vs Current practices

www.adselfserviceplus.com

# Table of contents

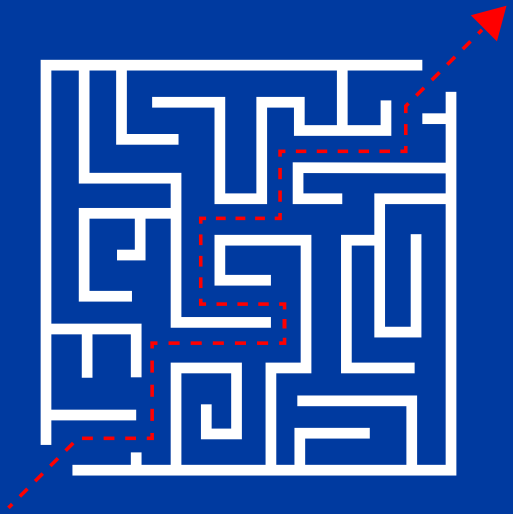
# What is the NIST?

The National Institute of Standards and Technology (NIST) is a non-regulatory agency that is funded by the United States' Department of Commerce. It has been in operation since 1901, and aims at providing security guidelines, quality standards, and more for various industries.

Over the years, the NIST has grown to become an authoritative voice on establishing standards and best practices on securing digital identities. Since the NIST is a federal agency, it regulates all the government organizations of the United States. It is mandatory for government agencies in the United States like the FBI, USDA, and NSA to adhere to NIST guidelines.

Let's take a look at what NIST password guidelines say, and how they compare with current password practices.

# 1. Password complexity



## What the NIST recommends

According to the NIST, longer passwords are better. According to NIST recommendations, passwords should contain at least eight characters and can be as long as 64 characters. The NIST also recommends using passphrases to encourage setting longer passwords.

## Current practice

For many organizations, the minimum length of 8 characters is pretty much the standard. However, many organizations limit password length to 16 characters.

Using ADSelfService Plus, admins can set the minimum and maximum length of passwords as recommended by the NIST, apart from setting various complexity rules to bolster the strength of passwords.

# 2. Periodic password reset

## What the NIST recommends

NIST says that periodic password resets have become counter-productive, as users end up setting weaker passwords to help with remembering them. This compromises the security of an organization. The NIST recommends resetting passwords only when necessary.

## Current practice

Generally, organizations have a password expiration policy that allows passwords to be 60 to 90 days old at max.

The NIST doesn't recommend password expiration due to the above mentioned reason. However, to prevent users from setting weak passwords, strong password rules can be set along with password expiration rules, so that the security provided by both practices remain in place. ADSelfService Plus can further allow you to set different password rules for different users based on your organization's needs.

# 3. Password screening

## What the NIST recommends

Screening passwords against a dictionary of commonly used passwords is a NIST recommendation. Guessing common passwords is one of the easiest ways for hackers to get inside an organization using brute force, which is why the NIST strongly recommends screening passwords.

## Current practice

Many companies do use some form of password screening to prevent the use of common passwords. However, this practice is not widespread.

ADSelfService Plus can not only screen passwords for dictionary words, it can also prevent other common practices such as using usernames or sequential characters in passwords, which greatly reduces the probability of passwords being weak.

# 4.

# Multi-factor authentication

## What the NIST recommends

NIST recommends two-factor authentication (2FA), but it discourages the use of SMS notification as an authentication factor and suggests using stronger processes such as Google Authenticator. This is due to the inherent security risks involved in using SMS.

## Current practice

The current trend is divided, with some organizations using 2FA or multi-factor authentication (MFA) while others don't use any kind of authentication process.

MFA plays a vital role in bolstering an organization's security. ADSelfService Plus can secure Windows, Mac, and Linux logons with 2FA and user accounts with MFA systems such as Google Authenticator and RADIUS authentication as recommended by the NIST.

# 5. Number of password attempts

## What the NIST recommends

NIST recommends allowing at least 10 attempts before locking an account. It takes a substantial amount of attempts to brute force into an account, unless the password is a common one like admin123. So, the NIST recommends a higher number of attempts to take some of the pressure off the user.

## Current practice

Many organizations limit the number of attempts to five, or sometimes even three. This gives very little leeway for the user, and increases the number of help desk tickets, and, incidentally, help desk costs.

A limited number of attempts is implemented, as there's a chance cybercriminals can brute force into accounts with weaker passwords. However, with ADSelfService Plus, strong password policies can be enforced that negate the opportunity for setting weak passwords, making such practices obsolete.

# Summary

NIST password guidelines are a robust set of recommendations that any organization can implement to fortify its security, and prevent costly compromises such as data breaches. Using solutions like ADSelfService Plus can make implementing NIST guidelines in your organization easy. Strong password management practices and security systems go a long way in protecting an organization from threats.

ManageEngine
ADSelfService Plus

ADSelfService Plus is an integrated self-service password management and single sign-on solution. It offers password self-service, password expiration reminders, a self-service directory updater, two-factor authentication for Windows logons, a multiplatform password synchronizer, and single sign-on for cloud applications. ADSelfService Plus' Android and iOS mobile apps, as well as Windows, macOS, and Linux login agents, facilitate self-service actions for end users anywhere, at any time.

$ Get Quote

⤓ Download